UPC - Departamento de Telemática

SEGURIDAD EN LOS PROCESOS DE VOTO ELECTRÓNICO REMOTO: REGISTRO, VOTACIÓN, CONSOLIDACIÓN DE RESULTADOS Y AUDITORIA.

Victor Manuel Morales Rocha

CONTENIDO

Capítulo 1

Introducción

Los procesos de votación datan de hace más de 2500 años y han sido parte fundamental en los procesos democráticos. El voto constituye un derecho de los ciudadanos y en algunos casos también una obligación. Los procesos de votación determinan los destinos de pueblos completos. Por esta razón, dichos procesos captan la atención de masas. En las democracias actuales se busca que los resultados de una elección representen la voluntad del pueblo, por lo cuál existe gran interés en que dichos resultados sean precisos y confiables.

La tendencia de los últimos años en los procesos electorales ha sido utilizar medios electrónicos para automatizar y hacer más eficientes los diferentes procesos de una elección. Aún cuando esta automatización se ha presentado de manera gradual, el propósito final es utilizar medios electrónicos para el registro de votantes, autenticación de los votantes registrados, emisión del voto, y desde luego para el escrutinio y publicación de resultados. Contrario a lo que en un principio pudo haberse planteado, algunos sistemas de votación electrónica han generado controversia debido a diferentes problemas que han surgido con su uso. Aún así, se continúa con la búsqueda de soluciones ya que en términos generales la automatización de los procesos de una elección aporta grandes ventajas.

En este capítulo se presentarán algunos conceptos básicos relacionados con elecciones, así como la forma en que la tecnología ha intervenido para tratar de llevarlas a cabo de

una manera más eficiente. Se describen además algunas experiencias relevantes alrededor del mundo, así como problemas que se han detectado por medio de dichas experiencias.

1.1 Modelo básico de elecciones

En un modelo básico de elecciones participan principalmente dos tipos de agentes: autoridades de la elección y votantes. Estos pueden ser definidos como sigue:

Autoridad de la elección
Es la persona o grupo de personas a cargo del proceso de elección. Dicha autoridad establece los parámetros del proceso, los requisitos de los participantes, el objetivo de la elección, etc.

Votante
Es cualquier persona que tiene derecho a participar en un proceso de elección emitiendo un voto. Una persona es un votante legítimo si cumple con los requisitos definidos por la autoridad de la elección.

Además de los agentes definidos, puede haber otros que participen en el proceso de elección, tal como proveedores de servicios para una o varias fases de la elección.

Se pueden definir entonces las fases en las que se desenvuelve un modelo básico de elecciones. Estas fases son:

- Preparación
    - Registro de votantes para definir el censo electoral
    - Anuncio de la elección
    - Definición de parámetros de la elección
    - Preparación técnica y configuración de la elección
- Votación

    - Autenticación
    - Envío del voto
- Consolidación de resultados
    - Recolección de votos
    - Escrutinio y determinación de resultados
    - Publicación de resultados

1.2 Tipos de elección

Existe una gran variedad de tipos de elección. Se describen a continuación las más comunes:

- Si / No. El votante debe escoger la respuesta a una pregunta cerrada. Las consultas ciudadanas o referendos entran en esta clasificación.
- 1 de N. El votante debe escoger una entre N opciones posibles.
- K de N. El votante debe escoger K (K>1) entre N opciones posibles.
- K de N con orden de preferencia. El votante debe escoger en orden de preferencia K (K>1) entre N opciones posibles.
- N de N ordenados por preferencia. El votante selecciona el total de las opciones en orden de preferencia.
- Abierta. El votante plantea su propia opción de voto. Este tipo de elección puede ser combinado con otros, por ejemplo con "1 de N", de forma que el votante puede escoger una entre N opciones posibles, o bien, proponer su propia opción.

1.3 Entornos de elección

Existen diferentes entornos en los cuáles se llevan a cabo procesos de elección. Los más conocidos son los entornos gubernamentales (elecciones presidenciales, parlamentarias,

municipales, etc.), sin embargo también se llevan a cabo elecciones en entornos a menor escala como son asociaciones estudiantiles, juntas de accionistas, sindicatos, etc.

1.4 Evolución del voto electrónico

El objetivo de los sistemas de votación electrónica es tratar de automatizar los diferentes procesos de la elección a fin de lograr una mayor eficiencia. Los primeros sistemas automatizados han estado enfocados al escrutinio de los votos. Sin embargo, también se han estado llevando a la práctica sistemas electrónicos para cada una de las fases de una elección, por ejemplo para el registro de los votantes y para la fase de votación.

A continuación se describe una breve reseña de la evolución de los sistemas de voto electrónico más importantes.

1.4.1 Sistemas de Reconocimiento Óptico de Marcas (OMR)

Estos sistemas emplean papeletas de votación en las cuáles los candidatos u opciones de votación están impresos junto con viñetas que pueden rellenarse. Los votantes escogen su opción rellenando la viñeta anexa a su preferencia. Al finalizar el proceso de votación, el votante coloca la papeleta en un dispositivo para que sea escaneada y de esta manera se confeccione en paralelo un registro electrónico de los votos. El votante también puede depositar la papeleta en una urna física, y en este caso sería un oficial de la elección (por ejemplo el presidente de la mesa electoral) quien coloque el conjunto de papeletas de votación en el dispositivo de escaneo al final de la elección. Utilizando esta tecnología se pueden obtener automáticamente los resultados locales de una elección. Para un escrutinio global, algunos de los dispositivos tienen la posibilidad de conectarse remotamente a un servidor central para realizar el envío de sus resultados locales. De otro modo, se emplean otros medios para llevar a cabo la recolección de los votos.

El dispositivo de escaneo utiliza técnicas de reconocimiento de marcas, en donde se tienen en cuenta las partes más oscuras del área destinada para rellenar los votos, deduciendo de esta manera las preferencias del votante. Esta es una tecnología ampliamente utilizada en otras áreas por lo que su correcta funcionalidad ha sido suficientemente probada.

1.4.2 Sistemas de Registro Electrónico Directo (DRE)

Estos sistemas de votación utilizan medios digitales para la selección del voto, por ejemplo, por medio de botones o pantalla táctil incluidos en el terminal de votación. El registro del voto se almacena localmente en formato electrónico. Los sistemas DRE previenen a los votantes de errores involuntarios, ya que el terminal de votación conduce al votante paso a paso hasta que un voto válido es registrado. Una variante de los sistemas DRE son los que imprimen la papeleta para que sea depositada en una urna, teniendo de esa manera un registro electrónico y otro impreso.

Los terminales DRE suelen contar con una interfaz de red, por lo que los resultados generados localmente pueden enviarse a un servidor central por medio de una red de comunicación. Otra opción es almacenar una copia de los resultados locales en un medio de almacenamiento removible y entonces enviar dicho registro a un centro de escrutinio para la consolidación de los resultados.

1.4.3 Sistemas de Voto Electrónico Remoto

Los sistemas de voto electrónico remoto surgen especialmente para tratar de dar al votante una mayor facilidad para emitir su voto al no tener que acudir a un lugar específico para emitir su voto. Si bien las características de los sistemas de voto remoto son atractivas, resultan más complejos que los sistemas de voto presencial debido a los riesgos de seguridad inherentes a un ambiente de votación remoto, en el cuál la autoridad de la elección no puede tener control. Existen diversos canales de comunicación en los

cuáles se puede llevar a cabo el voto remoto, entre los que se puede destacar Internet (Web o e-mail), SMS, IVR, etc. En el capítulo 3 se presenta una comparativa de los sistemas de voto remoto más utilizados, incluyendo voto postal.

1.5 Ventajas de los sistemas de voto electrónico

Las ventajas de los sistemas de votación electrónica sobre los sistemas tradicionales de votación en papel se destacan a continuación:

- Rapidez en el escrutinio de los votos.
- Accesibilidad para votantes con discapacidades físicas.
- Prevención de errores en el proceso de votación, lo cuál evita que se tengan que anular votos.
- Menores costos de implementación (en elecciones a gran escala y/o con el paso del tiempo).
- Posibilidad de que el votante pueda verificar el correcto tratamiento de su voto.

Por su parte, con el uso de un sistema de voto electrónico remoto existen algunas ventajas adicionales:

- Conveniencia para el votante, al no tener que desplazarse a un precinto de votación específico.
- Horario más amplio del período de votación, que puede ser de varios días o incluso semanas.
- Gestión centralizada del proceso de elección.

1.6 Experiencias alrededor del mundo

Se han llevado a cabo procesos de elección por medio de sistemas de votación electrónica (presenciales y remotos) en gran cantidad de países. La mayoría de estas

implementaciones sólo han sido parte de proyectos pilotos, principalmente debido a falta de legislación que permita el uso de tales sistemas para que los votos que se generan sean vinculantes al resultado de la elección en la que participan.

Se destacan a continuación las principales experiencias de voto electrónico remoto que se han llevado a cabo a la fecha en diferentes países.

Austria

En Austria se han llevado a cabo algunas experiencias de voto electrónico remoto. En mayo de 2003 se llevó a cabo la primera de ellas [Au03]. Esta primera experiencia se desarrolló en paralelo a las elecciones de la "Student Union Elections" de la Universidad de Viena para elegir a sus representantes estudiantiles. Se utilizó un prototipo desarrollado por el Profesor Prosser de la Universidad de Economía y Administración de negocios de Viena y su equipo de investigación denominado e-Voting. Para el acceso al sistema de votación se utilizó la tarjeta de identidad electrónica comúnmente utilizada en Austria.

En abril del 2004 se llevó a cabo el segundo proyecto [Au04] siguiendo las mismas características del proyecto del año anterior. En esta ocasión la votación electrónica remota se realizó de manera paralela a las elecciones presidenciales de Austria.

En el 2006 el grupo de investigación e-Voting llevó a cabo otra prueba de voto electrónico remoto para residentes en el extranjero [Au06]. Los votantes tenían que solicitar sus credenciales de votación para participar en la votación por Internet. El período de votación fue de 3 días (12 al 14 de octubre).

Ninguna de las experiencias llevadas a cabo hasta la fecha en Austria han sido vinculantes, por lo que sólo se pueden considerar como pruebas funcionales y técnicas de las plataformas utilizadas.

España

En noviembre del 2003, más de 23000 catalanes residentes en el extranjero (en Argentina, Bélgica, Estados Unidos, México y Chile) fueron invitados a participar en un piloto de votación por Internet [RB04a]. Este piloto se efectuó en paralelo a las elecciones del parlamento de Cataluña, en donde dichos votantes podían votar de manera vinculante por correo postal. Debido a problemas con el servicio postal, el material electoral destinado a parte de los residentes en México no pudo ser entregado a tiempo. Por esta razón, la participación de voto por Internet en dicho país excedió en más de un 200% al número de votos postales enviados.

El Ayuntamiento de Madrid organizó en junio de 2004 una consulta ciudadana destinada a probar diferentes aspectos del voto electrónico remoto [RB04b]. Para este propósito, se escogió un censo de aproximadamente 100000 personas correspondientes al Distrito Centro de Madrid que tuvieron la oportunidad de participar usando Internet o teléfono móvil como canales de votación. El número de personas que se registraron para participar en el piloto fue de 1351y el de votos emitidos fue de 882.

Posteriormente, entre el 1 y el 18 de febrero del 2005, cerca de dos millones de votantes de 52 municipios (un municipio de cada provincia) tuvieron la oportunidad de participar en un piloto no vinculante de voto por Internet [OVE05]. El piloto se realizó en paralelo con un sistema convencional de voto vinculante basado en papel para un referéndum de la constitución europea. De acuerdo a informes de prensa, 10543 votantes enviaron su voto por Internet.

Estonia

Estonia se caracteriza por ser un país en donde la tecnología de la información es ampliamente utilizada. Más de la mitad de los hogares cuentan con un ordenador y 4 de cada 5 ordenadores tienen una conexión a Internet. Además, los ciudadanos cuentan con

una identificación electrónica que almacena un certificado digital del ciudadano, el cuál es empleado para diversos trámites.

Estos antecedentes han permitido que Estonia sea el primer país que utilice Internet como uno de sus canales de votación para elecciones gubernamentales en donde los votos fueron vinculantes. La primera elección con estas características se llevó a cabo en las elecciones locales en octubre del 2005 [MM05]. En dicha experiencia 9287 votantes emitieron su voto por Internet, lo cuál representó el 1.9 % de los votos en total.

Posteriormente, en marzo del 2007 se volvió a utilizar Internet para las elecciones del parlamento [MH08]. En esta ocasión, hubo 30275 votantes que utilizaron Internet como medio de votación, lo cuál representó el 5.4 % del total de votantes que participaron y tres veces más la cantidad de votos emitidos en el 2005. Ambas experiencias han sido calificadas como exitosas y no han generado ningún tipo de controversia.

Estados Unidos de América

En el 2000, la FVAP (Federal Voting Assistance Program) llevó a cabo un programa piloto llamado VOI - Voting Over the Internet [VOI00] para probar la fiabilidad de Internet como canal de comunicación para el envío de los votos. Éste fue un piloto pequeño en el que pudieron participar algunos votantes voluntarios (menos de 100) de condados de Carolina del Sur, Florida, Texas y Utah. Después del experimento, la FVAP declaró que el piloto había sido un éxito y concluyeron que para voto remoto a pequeña escala, Internet era una buena alternativa para los residentes en el extranjero.

Después del éxito en el piloto del 2000, el Departamento de Defensa fue asignado para llevar a cabo un proyecto similar, pero éste a gran escala (proyecto SERVE). En este proyecto se esperaba que participaran cerca de 100000 votantes residentes en el extranjero en las elecciones primarias y generales del 2004. Sin embargo, debido a un informe [JRS+04] emitido por un grupo de académicos en el que se resaltaban los riesgos de seguridad al llevar a cabo elecciones por medio de Internet, el proyecto fue cancelado.

Las principales advertencias mencionadas en el informe se referían al riesgo de pérdida del anonimato del votante y a la posibilidad de manipulación del voto tanto en el terminal de votación como durante la transmisión.

En las elecciones primarias demócratas del 2008 se permitió a los residentes en el extranjero que se registraran y enviaran su voto a través de Internet. Posteriormente, para las elecciones generales del mismo año, el condado de Okaloosa en el estado de Florida llevó a cabo con éxito un piloto vinculante en el que los militares desplazados en ciertas bases militares de Alemania, Japón y Reino Unido pudieron votar a través de Internet. La plataforma utilizada en este último piloto fue evaluada exhaustivamente por un grupo de académicos en el área de seguridad con el fin de determinar los posibles riesgos durante la elección. En su informe [CHI+08], concluyeron que dicho sistema era seguro contra posibles ataques externos y que era más eficiente que los utilizados a la fecha para el envío de votos desde el extranjero, como el voto por fax, voto postal, etc.

Filipinas

Entre los meses de julio y agosto del 2007 se llevó a cabo un piloto de elecciones por Internet para los filipinos residentes en Singapur. Se instalaron terminales de votación en el consulado filipino en Singapur desde las que se podía enviar el voto. En este piloto se pretendía probar la usabilidad y seguridad del sistema, y al final de la elección la autoridad electoral del país declaró [Co07] que el sistema utilizado cumplía con ambas características aún cuando sólo se recibieron 311 votos.

Francia

En el 2001, en la pequeña población francesa llamada Voisins-le-Bretonneux se llevaron a cabo las elecciones del municipio y del cantón desde kioscos con conexión a Internet. Posteriormente, en Noviembre del 2002, se volvió a utilizar Internet como canal de votación en la localidad de Issy-les-Moulineaux para las elecciones locales. En mayo del 2003, los franceses residentes en los Estados Unidos tuvieron la posibilidad de elegir a

los representantes de la asamblea de los ciudadanos franceses en el extranjero (AFE) a través de Internet. Ese mismo año, el "Internet Rights Forum" [IRF08], un grupo privado soportado por el gobierno francés, publicó algunas recomendaciones [Fr03] acerca del futuro del voto electrónico en Francia. Entre sus recomendaciones declararon que el voto electrónico remoto no debería ser utilizado, excepto en los casos de los residentes en el extranjero para elegir a sus representantes.

El sitio Web francés Ordinateurs-de-vote.org ha formulado una petición al gobierno de que se preserve el voto en papel, o en otras palabras, que no se utilice voto electrónico en ninguna de sus formas. Para Octubre del 2008, se habían reunido más de 103000 firmas [Or08]. Sin embargo, algunos oficiales del gobierno francés están buscando introducir el voto por Internet al alcance de todos los votantes para el 2009.

Reino Unido

A partil de 1997 el gobierno británico ha llevado a cabo acciones para introducir el voto electrónico en el país. Estas acciones han incluido algunos pilotos en los que se utiliza el voto electrónico remoto. En mayo del 2002 se experimentó con voto por teléfono, Internet y mensajes de texto por teléfono móvil. Al año siguiente se volvieron a implementar pilotos semejantes y se esperaba que para el 2004 el alcance de los pilotos se extendiera a algunos millones de votantes para las elecciones al parlamento europeo. Sin embargo, la Comisión Electoral recomendó en su informe para dichas elecciones que no se llevaran a cabo pilotos de voto electrónico por considerar que las regiones que participarían no estaban listas para este tipo de innovaciones.

El 29 de enero del 2007, el gobierno anunció [Uk07a] que se llevarían a cabo nuevos pilotos para las elecciones locales del 3 de mayo de ese año en 12 localidades diferentes. Para agosto del 2007, debido a los informes de dichos pilotos, la Comisión Electoral hizo un llamado [EC07] a que se diera fin a los pilotos de voto electrónico hasta que el gobierno pudiera establecer una estrategia de modernización del sistema electoral que hiciera el voto electrónico más seguro.

Suiza

Siendo que Suiza tiene una política de gobierno que involucra frecuentemente la participación ciudadana para tomar decisiones en cuanto a la manera de gastar el presupuesto público, el uso del voto electrónico remoto ha sido de gran utilidad. En un sitio Web del gobierno Suizo [FOC] se describen las experiencias que han tenido con el uso del voto electrónico. Cabe destacar, que para los suizos, el término voto electrónico se refiere específicamente al voto llevado a cabo desde medios electrónicos remotos como Internet.

Los votantes del cantón de Ginebra, en la comunidad de Anières fueron los primeros en participar en una experiencia de voto electrónico en Suiza. Dicha experiencia se llevó a cabo el 19 de Enero del 2003. En los meses siguientes, otras comunidades del cantón empezaron a adoptar el mismo sistema de voto electrónico, el cuál está basado en Internet [CdG03].

En el cantón de Neuchâtel se ha creado un concepto para los ciudadanos que consiste de un identificador de usuario, una contraseña y códigos de transacción. Dicho concepto permite el acceso a una variedad de servicios gubernamentales, entre ellos el voto electrónico remoto basado en Internet.

Por su parte, Zurich ha creado una base de datos de votantes compartida entre las comunidades del cantón. Esta ha sido utilizada en voto electrónico desde diciembre del 2004. La votación se lleva a cabo por Internet a través de un sitio Web ya establecido para ese fin [KZ08] o a través de mensajes de texto vía teléfono móvil.

1.7 Planteamiento del Problema

Una parte importante de los sistemas electrónicos de votación es que con ellos se trata de mitigar los problemas comunes del voto tradicional en papel. Actualmente, las nuevas

tecnologías de comunicación y los protocolos criptográficos pueden aplicarse a la automatización de los procesos de elección. Además, esta automatización debe preservar e incluso aumentar la seguridad de las elecciones convencionales.

A continuación se describen los principales aspectos de una elección que presentan vulnerabilidades importantes y que han impedido el uso extensivo del voto electrónico:

- Si bien la mayoría de las propuestas de esquemas de voto electrónico se concentran en la fase de votación, es importante considerar que existe una fase previa en la que se constituye el censo electoral. Si la recopilación de dicho censo no se lleva a cabo de una manera eficiente y segura, puede haber consecuencias negativas en las fases posteriores. Este proceso de recolección de datos de votantes le denominamos "registro de votantes" y es parte de la preparación de una elección. En los últimos años, en algunos países, se han empezado a utilizar medios remotos para llevar a cabo este proceso de una manera más eficiente. Sin embargo, los sistemas actuales de registro remoto de votantes presentan algunos riesgos de seguridad que pueden resultar en un censo electoral deficiente.

- Tradicionalmente en unas elecciones gubernamentales que utilizan un sistema de votación basado en papel, el votante marca su opción de voto, deposita la papeleta en una urna y ahí termina su función. El votante no tiene forma de verificar que en el escrutinio su voto se ha incluido correctamente, aún cuando al final de la elección se publique una lista con los nombres de los votantes que ejercieron su derecho al voto. Por lo tanto, los votantes tienen que confiar en la autoridad de la elección cuando se publican los resultados de la elección. Por su parte, en muchos de los esquemas de voto electrónico propuestos a la fecha no se considera la verificación por parte del votante como parte fundamental de la seguridad, es decir, el votante no cuenta con mecanismos eficientes que le permitan verificar que su voto se ha registrado correctamente y que en el escrutinio, dicho voto se ha incluido apropiadamente. Estos esquemas asumen que las autoridades de la elección y administradores de sistemas actuarán honestamente, y que los votantes

confían en dichas autoridades. En un ambiente real no podemos suponer eso, por lo que el votante necesita un medio de confianza tangible para que un sistema de voto sea fiable, y por tanto factible para su implementación. Por lo tanto, tendríamos que dividir la seguridad de un sistema de voto electrónico en dos aspectos. Por una parte, la seguridad que es auditada y validada por expertos en seguridad y que pueden constatar que cierto esquema cumple con los requerimientos de seguridad críticos. Por otro lado, se debe considerar la seguridad desde el punto de vista de los votantes, o dicho de otro modo, la percepción de seguridad y por lo tanto la fiabilidad que tienen los votantes en un sistema. Para lograr este segundo aspecto de seguridad, el sistema debe ser capaz de proporcionar al votante mecanismos de verificación que proporcionen dicha confianza.

- Además se presenta el problema de consolidar los resultados de una elección para llevar a cabo el escrutinio, especialmente cuando la elección se lleva a cabo utilizando distintos canales de votación. Por ejemplo, en una elección se podrían utilizar simultáneamente máquinas de votación de registro directo (DRE's), voto convencional en papel, voto postal y voto por Internet. A la hora de consolidar los resultados a partir de los distintos canales de votación se presentan serias complicaciones de seguridad que podrían llegar a alterar los resultados reales.

- Un problema adicional de los esquemas de voto electrónico, y de alguna manera paralelo al de la falta de mecanismos que permitan la verificación por parte del votante, es la falta de transparencia en la mayoría de los sistemas actualmente utilizados. Por esta razón, se requiere implementar técnicas que proporcionen elementos suficientes para llevar a cabo auditorias, dando de esta manera mayor transparencia y por lo tanto mayor confianza a los votantes.

Existe aún mucho por resolver entre los aspectos que proporcionan seguridad y eficiencia en los esquemas de voto electrónico remoto para que estos sean fiables ante la ciudadanía

en general. Por esta razón, con esta investigación se pretende contribuir en el aspecto de seguridad con el fin de dar un paso más hacia el uso extensivo de tales sistemas.

La presente investigación se realizó con el apoyo de una beca del fondo FIE (Formación de Investigadores en las empresas) gestionado por AGAUR (Agència de Gestió d'Ajuts Universitaris i de Recerca de la Generalitat de Catalunya), como parte de un proyecto de investigación en la empresa Scytl Secure Electronic Voting. Aún cuando el aspecto principal tratado en esta tesis es la seguridad en los diferentes procesos de una elección, debido al entorno empresarial de desarrollo de esta investigación se han tenido en cuenta otros aspectos como son: usabilidad, viabilidad práctica y posibilidad de explotación mediante patentes.

1.8 Organización de la Tesis

El capítulo 2 describe los principales conceptos de criptografía aplicable a los distintos procesos del voto electrónico.

El capítulo 3 está dedicado a analizar los diferentes sistemas de voto remoto así como los requisitos de seguridad que se deben considerar en dichos sistemas. Se describe también la dificultad para satisfacer algunos de esos requisitos, especialmente en el voto electrónico remoto. También se analizan algunas de las principales amenazas de seguridad que afrontan los sistemas de voto electrónico remoto. Posteriormente se lleva a cabo un estudio comparativo de los diferentes sistemas de voto remoto y para concluir se describe un esquema de votación que permite una transición gradual hacia el voto remoto por Internet.

En el capítulo 4 se introducen los diferentes esquemas criptográficos de voto electrónico remoto, se analizan sus ventajas y desventajas y se presenta una comparación de dichos esquemas.

El capítulo 5 muestra la complejidad en la generación de un censo electoral a través de medios remotos de comunicación. Se propone en este capítulo un sistema de registro remoto de votantes que logra constituir un censo electoral de una manera fiable. Para lograrlo, se hace uso de algunas técnicas criptográficas y biométricas.

El capítulo 6 está enfocado en la verificación del voto por parte del votante (verificación individual). Se analizan diferentes propuestas y se proponen dos esquemas de votación que incluyen mecanismos para que el votante pueda verificar el correcto tratamiento de su voto.

En el capítulo 7 se propone un método de consolidación de resultados de una elección. El método propuesto se puede aplicar al voto electrónico remoto e incluso a los casos en los que la elección se lleva a cabo por distintos canales de votación (presenciales o remotos). Se utilizan técnicas criptográficas para proteger los resultados generados en cada uno de los canales de votación o unidades electorales y para una transferencia segura de dichos resultados hacia un servidor de consolidación.

Finalmente, en el capítulo 8 se describen los diferentes procesos de auditoria utilizados para los sistemas de voto electrónico. Se propone un mecanismo de auditoria que permite corroborar el correcto funcionamiento de un sistema de voto electrónico remoto, especialmente para detectar la inserción de votos ilegítimos por parte de atacantes internos o externos. El mecanismo se basa en el uso de criptografía para la protección de los votos una vez que estos han sido recibidos por el servidor de votación.

En la figura 1.1 se muestran las fases principales de una elección y los procesos generales que serán tratados en esta tesis.

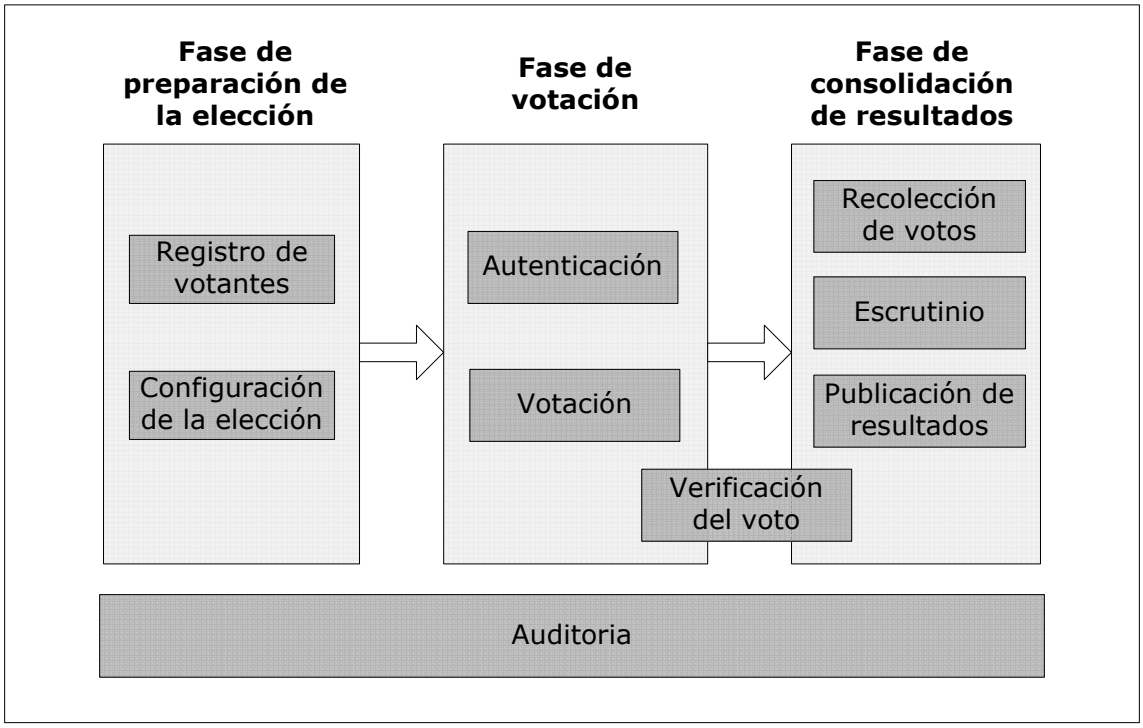

Figura 1.1. Procesos llevados a cabo en una elección

Capítulo 2

Primitivas de Criptografía

2.1 Criptografía en el voto electrónico

El voto electrónico presenta importantes retos en tres áreas principales: tecnológica, social y legislativa. A su vez, el principal reto tecnológico del voto electrónico es la seguridad. Es en este campo en donde la criptografía juega un papel central. A lo largo de las últimas dos décadas se han desarrollado protocolos criptográficos aplicables al voto electrónico. La primera propuesta de seguridad para el voto electrónico fue la de Chaum [Ch81]. El esquema propuesto, conocido como mix-net, fue en principio diseñado para la privacidad en el correo electrónico, sin embargo otra de sus aplicaciones se refiere a la privacidad de los votantes en un sistema de votación electrónica.

Algunos de los trabajos posteriores de voto electrónico han partido de la propuesta en [Ch81]. Sin embargo, ha habido otras variantes que también proponen el uso de la criptografía como parte central de un esquema de votación electrónica.

Los requerimientos de seguridad del voto electrónico que se tratan de satisfacer por medio de criptografía son: privacidad de los votos, autenticación de los votantes e integridad de los elementos de la elección.

En las siguientes secciones se describen los mecanismos criptográficos específicos en los entornos de votación electrónica. Se asume que el lector tiene conocimiento previo de los

fundamentos de la criptografía y de sus aplicaciones básicas, por lo que aquí no serán detallados. Se pueden consultar dichos conceptos en diferentes fuentes, por ejemplo [Sc96, MOV01].

2.2 Firma ciega

Existen aplicaciones en las que se desea obtener una firma digital sin que el firmante tenga conocimiento del contenido del mensaje a firmar. Esto se puede lograr por medio de una firma ciega [Ch82], en la que se aplica una función matemática sobre el mensaje a firmar con el fin de modificarlo. El factor utilizado en la función matemática es comúnmente llamado "factor de cegado" y es un valor generado de manera aleatoria.

La firma ciega debe cumplir con algunas características, entre ellas:

- La firma resultante puede ser públicamente verificada, tal como las firmas digitales regulares.
- El firmante no puede deducir el contenido del mensaje firmado tomando como base el momento en que se llevó a cabo la firma.

Un esquema de firma ciega puede llevarse a cabo por medio de esquemas comunes de firma digital con criptografía pública, por ejemplo con RSA. En este caso, un esquema de firma ciega [Ch85] funcionaría de la siguiente manera:

1. El autor del mensaje M calcula de manera aleatoria el factor de cegado k.

2. El autor ciega el mensaje M:
$$M' = Mk^e \bmod n$$

3. El firmante recibe M' y lo firma:
$$M'^d = (Mk^e)^d \bmod n$$

4. El autor desvela M'^{d} calculando:

$$F = M'^{d} / k \bmod n$$

obteniendo como resultado:

$$F = M^{d} \bmod n$$

es decir, el mensaje M firmado digitalmente.

2.3 Esquemas de secreto compartido

Para asegurar la protección frente a pérdidas de un secreto, la primera opción sería tener respaldos de dicho secreto. Sin embargo, mientras más respaldos existan, mayor es el riesgo de que el secreto sea comprometido. Por otro lado, si hay menos respaldos, será mayor el riesgo de pérdida. Los esquemas de secreto compartido permiten aumentar la disponibilidad del secreto sin incrementar el riesgo de compromiso

El propósito de los esquemas de secreto compartido es proteger un secreto frente a posibles pérdidas y distribuir la confianza del secreto entre varios participantes. Esta distribución se consigue "dividiendo" el secreto en distintas partes que son repartidas entre los participantes, de tal forma que sólo con la colaboración de un conjunto de dichos participantes, se puede reconstruir dicho secreto.

Por su parte, un esquema umbral de secreto compartido $(t;n)$ es un método para compartir un secreto S entre n usuarios de forma que la colaboración de cualquier subconjunto t de usuarios es útil para recuperar S. Sin embargo, ningún subconjunto de $t-1$ o menor puede recuperar S. Además, conociendo las partes de sólo $t-1$ no debe dar indicios para deducir el secreto. Este concepto de secreto compartido umbral se debe a Shamir [Sh79] y su funcionamiento está basado en interpolación polinomial y en el hecho de que una función polinomial univariada $y = f(x)$ de grado $t-1$ quede definida de forma unívoca por t puntos (x_i, y_i) con distinto x_i.

Los esquemas de secreto compartido son muy útiles para la administración de claves. El concepto consiste en dividir una clave privada entre varios participantes, de tal manera que el uso de la clave dependa de la colaboración de los participantes. Por ejemplo, una clave privada se puede dividir en 10 partes para ser repartidas entre 10 participantes y se requiere que al menos 5 de ellos colaboren para recuperar la clave. También se pueden definir dos o más grupos de participantes de tal manera que cierto número de participantes de cada grupo deba colaborar para reconstruir la clave.

Con dicho concepto de secreto compartido, una clave privada se confía a un conjunto de participantes, lo cuál previene problemas de protección o recuperación de la claves.

2.4 Pruebas de conocimiento nulo

Consideremos dos entidades *P* (probador) y *V* (verificador) que desconfían la una de la otra. *P* posee un secreto *s* y quiere probar a *V* la posesión de ese secreto sin revelarle el contenido. Un protocolo de pruebas de conocimiento nulo permite a *P* probar a *V*, a través de un proceso interactivo, que posee el secreto *s*. Este proceso no revela el contenido de *s*.

El protocolo consiste en que *V* genera una serie de preguntas o retos que *P* sólo podrá responder si realmente posee el secreto *s*. En caso de no poseer *s*, *P* sólo podrá responder correctamente a cada pregunta con una probabilidad de ½. Por lo tanto, entre más preguntas se incluyan en el proceso de prueba, menor será la probabilidad de que *P* engañe a *V*.

El protocolo podría ser definido como se describe a continuación. A fin de que *P* pueda demostrar que se encuentra en posesión del secreto *s*, construye un problema matemático *m* que sea computacionalmente difícil de resolver, de forma que *s* sea una solución para *m*. Entonces se llevan a cabo las siguientes operaciones:

1. *P* transforma *m* para obtener un nuevo problema matemático *m*', cuya solución *s*' se puede calcular fácilmente a partir de *s*.
2. *P* envía *m*' a *V*.

3. *V* genera un bit aleatorio *b* y lo envía a *P*.

4. El valor de *b* determina el reto:
    - Si *b* = 0, *P* demuestra la relación entre *m* y *m*', sin dar la solución de *m*'.
    - Si *b* = 1, *P* proporciona la solución s' del problema *m*' sin revelar la relación entre *m* y *m*'.

La única forma de que *P* responda correctamente ambos retos es poseyendo el secreto *s*.

2.5 Mix-nets

El propósito de las mix-nets (redes de mezclado o permutación) es crear un canal de comunicación anónimo con el fin de preservar la privacidad de los participantes en una comunicación. El origen de las mix-nets se remonta al concepto creado por Chaum [Ch81], el cuál fue originalmente creado para lograr anonimato en el envío de correo electrónico.

Una mix-net se compone de uno o más servidores, llamados servidores mix. El primer servidor mix recibe a través del tiempo mensajes de entrada provenientes probablemente de distintos emisores, los permuta de manera aleatoria y les aplica una función de transformación que puede ser de descifrado (mix-net de descifrado) o re-cifrado (mix-net de re-cifrado) y en un momento determinado reenvía los mensajes permutados y transformados al siguiente servidor mix. La misma operación de permutación y cifrado es repetida en cada servidor mix hasta que los mensajes son recibidos por el servidor final. La figura 2.1 muestra un ejemplo de una mix-net.

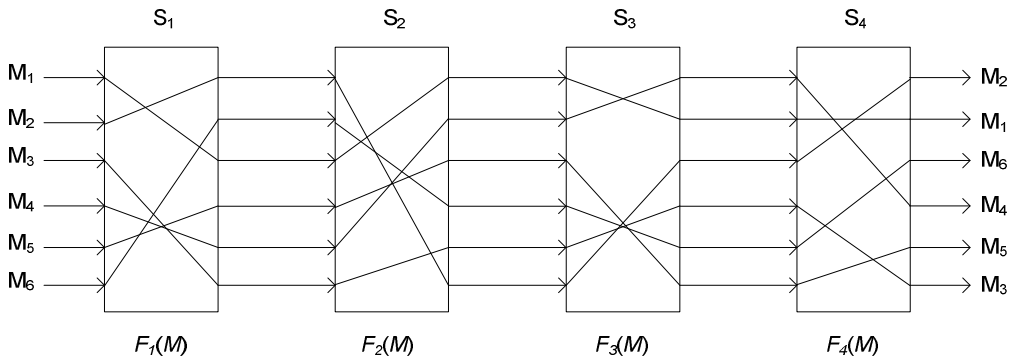

Figura 2.1. Ejemplo de mix-net con 4 servidores mix que reciben como entrada 6 mensajes

Una mix-net permite conservar el anonimato del emisor de un mensaje dado, lo cuál se logra por medio de la permutación de mensajes que realiza cada servidor mix. Podemos afirmar entonces que un servidor mix honesto es suficiente para lograr anonimato, ya que para un observador resulta igualmente probable que un mensaje saliente provenga de cualquiera de los mensajes entrantes y por tanto de cualquiera de los emisores participantes. Sin embargo, un mayor número de servidores mix evitará la pérdida de anonimato que supondría el compromiso de un servidor mix. Por otro lado, mientras más grande es el conjunto de mensajes operados en la mix-net, mayor es el grado de anonimato.

En una mix-net de descifrado, el emisor debe cifrar el mensaje tantas veces como número de servidores mix participan. El cifrado se lleva a cabo utilizando las claves públicas de los servidores mix en el orden inverso a la trayectoria del mensaje. De esta manera se forma un cifrado anidado el cuál se irá descifrando a medida que recorra los diferentes servidores. El primer servidor utiliza su clave privada para descifrar la parte que le corresponde de los mensajes recibidos, entonces lleva a cabo la función de permutación y reenvía los mensajes al siguiente servidor. Esta operación es repetida hasta que se recuperan los mensajes originales.

Por su parte, en una mix-net de re-cifrado, el emisor del mensaje solamente tiene que cifrarlo una vez, utilizando una clave pública. Cuando el mensaje cifrado es recibido por el primer servidor, este lo vuelve a cifrar con la misma clave pública, lo permuta entre el resto de mensajes y los envía al siguiente servidor. Para descifrar el mensaje se utiliza la clave privada que corresponde a la clave pública que se utiliza para el cifrado. Criptosistemas como ElGamal [El84] permiten llevar a cabo esta tarea de re-cifrado y cifrado en un solo paso.

Podemos encontrar diversas propuestas de mix-nets en la literatura, véase por ejemplo [Ab98 y Ab99].

2.6 Cifrado homomórfico

Sea un esquema de cifrado probabilístico en donde:

- P es el espacio de mensajes en claro y,
- C es el espacio de mensajes cifrados;

tal que P es un grupo bajo la operación binaria $\oplus$ y C es un grupo bajo la operación $\otimes$.

La instancia E del esquema de cifrado probabilístico es creado mediante la generación de sus claves públicas y privadas.

- $E_r(m)$ es la función que denota el cifrado del mensaje m usando el parámetro r en la instancia E.
- r es un valor aleatorio usado en el cifrado.

Se puede decir que el esquema de cifrado probabilístico es homomórfico, si para cualquier instancia E del esquema de cifrado, dado $c_1 = E_{r1}(m_1)$ y $c_2 = E_{r2}(m_2)$, existe una r tal que:

$$c_1 \otimes c_2 = E_r(m_1 \oplus m_2)$$

Diversos criptosistemas pueden utilizar las propiedades homomórficas aditivas, entre ellos, ElGamal [El84], Paillier [Pa99], y algunas generalizaciones de RSA [DJ01].

Por ejemplo, en el criptosistema ElGamal tenemos que:

P es un conjunto de enteros módulo p ($P = Z_p$), y
C es un conjunto de pares $C = \{(a,b) \mid a,b \in Z_p\}$

La operación $\oplus$ es una multiplicación módulo p.

Para la operación binaria $\otimes$ definida en los textos cifrados se lleva a cabo la multiplicación módulo p por componentes. Dos mensajes en claro m_0 y m_1 son cifrados como:

$$E_{k0}(m_0) = (g^{k0}, h^{k0} m_0),$$
$$E_{k1}(m_1) = (g^{k1}, h^{k1} m_1),$$

donde k_0 y k_1 son valores aleatorios. Se tiene que:

$$E_{k0}(m_0)\, E_{k1}(m_1) = (g^{k0} g^{k1}, h^{k0}\, h^{k1} m_0 m_1) = (g^k, h^k m_0\, m_1) = E_k(m_0\, m_1),$$

para $k = k_0 + k_1$.

Por lo tanto, en el criptosistema ElGamal la multiplicación de los mensajes cifrados es equivalente a la multiplicación cifrada de sus correspondientes mensajes en claro.

Capítulo 3

Sistemas de Voto Remoto

3.1 Introducción

El propósito principal de los sistemas de voto remoto es proporcionar un medio de votación a los votantes que no tienen la posibilidad de acudir a un recinto de votación el día de la elección. Las razones de no poder acudir al recinto de votación pueden ser variadas, por ejemplo los votantes que residen en el extranjero, o votantes que viven en zonas muy alejadas a un recinto de votación.

Algunos países han implementado el uso del voto postal para permitir a los votantes emitir su voto de una manera remota. Sin embargo, debido a problemas comunes en los servicios postales para enviar el material a los votantes así como para recibir el voto, las autoridades electorales se han visto en la necesidad de estudiar vías alternas de votación remota, especialmente a través de medios electrónicos. En algunos casos ya se han estado implementando sistemas electrónicos de votación remota, por ejemplo en los Estados Unidos [AHR07], Suiza [Re08], Reino Unido [Uk07b] o Estonia [Es05].

En general, el voto electrónico remoto puede resultar más conveniente que el voto postal. Los votantes tienen menos restricciones en cuanto al tiempo en que deben enviar su voto. Además, un votante puede verificar de una manera rápida, incluso en tiempo real, si su voto ha sido recibido por la autoridad electoral. Por otro lado, en algunos sistemas como el voto por Internet, el votante es alertado si no completa de manera correcta la selección de un voto, lo cuál evita errores involuntarios que en el caso del voto en papel anularían

el voto. A pesar de dichas ventajas, la preocupación acerca de la seguridad en los medios electrónicos de votación ha evitado que su adopción se lleve a cabo de una manera más extensa.

En el caso específico de los Estados Unidos, algunos estados han implementado sistemas electrónicos de votación remota como una alternativa al voto postal para votantes residentes en el extranjero [Us07]. En este capítulo se describirán los sistemas de voto remoto actualmente usados en algunos países. Primeramente será descrito el voto postal ya que actualmente éste es el medio mas común para llevar a cabo votaciones remotas. Entre los sistemas electrónicos analizados se encuentran el voto por fax, el voto a través de correo electrónico y el voto por Internet. La figura 3.1 muestra una clasificación de los sistemas de votación analizados.

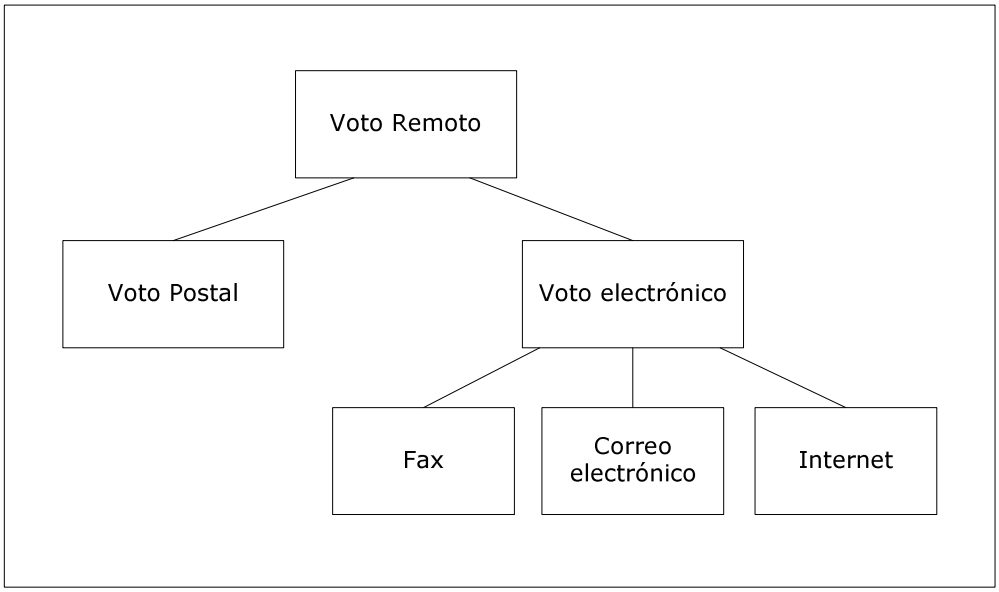

Figura 3.1. Clasificación de los sistemas de voto remoto analizados

Cabe resaltar que las desventajas principales de cualquier sistema remoto de votación son los riesgos de violación de la privacidad y la posibilidad de coerción o venta de votos, sin importar si el sistema se basa en papeletas (voto postal) o en medios electrónicos de transmisión [KV05].

3.2 Voto postal

Según lo define Qvortrup [Qv05]: "El voto postal es el uso del servicio postal como una alternativa para emitir los votos. En lugar de tener un solo día para que los votantes acudan a un recinto electoral para emitir sus votos, ellos reciben una papeleta por correo postal y entonces cuentan con un período el cuál deben regresar su voto por correo". En el voto postal, los votantes usualmente introducen su voto en un sobre. Este sobre a su vez es introducido en un segundo sobre en donde se incluye un certificado del votante, el cuál contiene los datos de identificación. En ocasiones el votante debe incluir su firma manuscrita como prueba de identificación. El segundo sobre es enviado a la autoridad de la elección a través de correo postal.

Tal como se puede ver en algunas experiencias descritas en [AHR07 y Uh05], en el voto postal existe el riesgo de retrasos tanto en el material que se envía al votante como en el voto enviado por el votante a la autoridad de la elección. Estos retrasos se deben principalmente a problemas en el servicio postal. Si el material de votación no llega a tiempo al votante, éste no tendrá la opción de enviar su voto y posiblemente sea tarde para llevar a cabo su votación de otra manera. Si el retraso se presenta en el retorno de la papeleta a la autoridad electoral, dicha papeleta no será incluida en el escrutinio de los votos. Este tipo de fallas es el principal problema de este canal de votación ya que causan que ciertos votantes se queden sin participar en la elección.

Además de los problemas ya mencionados, los votos enviados por correo postal están sujetos a manipulación durante su transporte. Los votos pueden ser modificados o incluso eliminados por adversarios que logren tener acceso a ellos. Existen propuestas basadas en códigos de seguimiento como se describe en [Vo08], que permiten saber si el voto ha llegado a la autoridad de la elección. Sin embargo, esto no resuelve el problema de la manipulación de los votos.

3.3 Voto electrónico remoto

Los sistemas de voto electrónico remoto se han estado utilizando y evaluando principalmente con el propósito de proporcionar una opción de emitir su voto a los votantes que no pueden acudir a votar presencialmente y como una alternativa al voto postal.

3.3.1 Voto por Fax

El voto por fax es aceptado por 24 estados en los Estados Unidos [Us07] y consiste en la transmisión de la papeleta con las opciones de votación marcadas a un número de fax previamente asignado [Fv06]. Este canal de votación es normalmente sugerido para contingencias en los casos en dónde el votante no ha podido emitir su voto a tiempo a través de otro medio.

La ventaja del voto por fax es que resuelve la incertidumbre que presenta el voto postal en cuanto a si el voto llegará a tiempo a la autoridad de la elección. Si la transmisión del fax es exitosa, el votante puede estar seguro que su voto ha llegado a la autoridad de la elección. Por otro lado, es evidente que el problema principal del voto por fax es la privacidad del votante. El voto se transmite a través de un canal inseguro junto con la identidad del votante, por lo que el contenido del voto es conocido cuando es recibido por la autoridad de la elección o aún si un atacante logra interceptar la comunicación. Una medida tomada para resolver este problema es separar la identidad del votante del contenido del voto cuando estos son recibidos y una vez que la identidad del votante ha sido comprobada como legítima. Sin embargo, esta medida sólo protege la privacidad cuando esta realmente ya pudo haber sido violada. Los estados que permiten el voto por fax solicitan a los votantes una declaración firmada de que renuncian a la privacidad de su voto.

3.3.2 Voto por correo electrónico

El voto por correo electrónico es utilizado en 7 estados de los Estados Unidos [Us07]. El proceso consiste en que el votante envía un correo electrónico con su papeleta escaneada como archivo adjunto. El mensaje es enviado a una dirección de correo electrónico establecida por la autoridad de la elección. Cuando el correo electrónico es recibido, se verifica la legitimidad del votante por medio de sus datos de identidad y si este es un votante válido se imprime la papeleta adjunta al correo. Dicha impresión es entonces puesta en un sobre para mantenerla segura hasta el proceso de escrutinio.

Al igual que en el voto por fax, los votantes deben firmar una renuncia a la privacidad de su voto [Fv06]. Por lo tanto, la principal desventaja del voto por correo electrónico, al igual que el voto por fax, es la violación de la privacidad ya que los contenidos de la papeleta son enviados junto con los datos de identidad del votante. Además, el envío del voto por correo electrónico posee un nuevo riesgo. Siendo el canal de transmisión de acceso público, se presenta la facilidad de un ataque de escuchas (eavesdropping) o de manipulación del contenido. Además, la confirmación de que un voto se ha recibido correctamente puede verse retrasada por problemas propios de la red. Esto coloca al voto por correo electrónico en una posición de fiabilidad intermedia comparándolo con el voto postal y el voto por fax. La confirmación de recepción del voto puede no ser inmediata, sin embargo será mucho más rápida que en el caso de voto postal. Esto proporciona la ventaja de saber que el voto debe ser enviado nuevamente si no se ha recibido.

3.3.3 Voto por Internet

En el informe "Internet Voting Report of the California Internet Voting Task Force" [Ca00] se ofrece la siguiente definición de voto por Internet: "un sistema de votación por Internet es definido como un sistema de elección que utiliza medios electrónicos que permiten a los votantes transmitir su voto a los oficiales de la elección a través de Internet".

El voto por Internet fue utilizado en el año 2000 por 4 estados de los Estados Unidos cuando el FVAP (The Federal Voting Assistance Program) llevó a cabo un proyecto piloto para las elecciones presidenciales [VOI00]. En el 2004, se pretendía llevar a cabo un proyecto similar pero aún de mayor alcance. El proyecto fue cancelado como consecuencia de un informe de evaluación de seguridad llevado a cabo por algunos académicos [JRS+04]. En este informe los autores resaltan que el uso de terminales de votación inseguros tales como los ordenadores personales y el diseño inseguro de Internet conlleva importantes riesgos de privacidad, integridad y fiabilidad para el proceso de votación. Los riesgos de privacidad e integridad descritos se atribuyen principalmente a la introducción de virus u otro tipo de software malicioso en el terminal de votación. Por su parte, los riesgos de fiabilidad se deben principalmente a la posibilidad de ataques de denegación de servicio, suplantación de identidad o de intermediario que suelen darse con frecuencia en Internet.

Por otro lado, el voto por Internet comparte las mismas ventajas de los sistemas de voto remoto descritos previamente. Además, el hecho de que el votante cuente con un medio interactivo para emitir su voto provee ventajas adicionales tales como la prevención de errores involuntarios. También permite el uso de protocolos criptográficos que resuelven el problema que presentan los demás esquemas de voto electrónico remoto en cuanto a la privacidad de los votantes. El uso apropiado de tales medidas criptográficas reduce la posibilidad de riesgos en el voto por Internet.

Los riesgos descritos en [JRS+04] son exclusivos del voto por Internet. Sin embargo, es importante notar que los otros canales de voto remoto descritos previamente también son susceptibles a ataques que podrían tener un efecto a gran escala en una elección. Por ejemplo, las papeletas enviadas por correo postal pueden ser interceptadas durante su transporte y por lo tanto pueden ser eliminadas o manipuladas. Uno de los objetivos del estudio presentado en la sección 3.8 es encontrar similitudes de los riesgos de seguridad que se presentan en cada uno de los sistemas de voto remoto y de esa manera facilitar la evaluación del impacto de esos riesgos.

3.4 Requisitos de seguridad

Es importante hacer notar que los sistemas de voto electrónico remoto deben satisfacer al menos los mismos requisitos de seguridad propios de los sistemas electrónicos presenciales, y aún los de los sistemas de voto convencional basado en papel. Diversos autores han descrito diferentes requisitos de seguridad [JE01, Ge01, FOO92, IIN01, SS04, CGS97], de los cuáles se puede obtener una visión global suficientemente amplia.

En resumen, los requerimientos que debe cumplir un sistema de voto electrónico remoto son los siguientes:

- *Legitimidad del votante*. En un proceso de elección, solamente pueden participar votantes autorizados y además sólo se puede tomar en cuenta un voto por votante. Tanto en los procesos de elección convencionales, como en los procesos que se utilizan sistemas de voto electrónico presencial, este requisito se cumple cuando el participante muestra una identificación que lo acredite como votante autorizado. La autoridad de la elección comprueba la legitimidad del votante verificando que su registro se encuentra en las listas del censo electoral. En el voto electrónico remoto es más complejo realizar dicha autenticación del votante. Comúnmente se han estado utilizando técnicas de identificación remota, por ejemplo un nombre de usuario y contraseña o certificados digitales.

- *Privacidad*. La relación entre votante y voto no debe ser conocida ni deducida. En un proceso de voto convencional se logra ocultar fácilmente la opción elegida por un votante, ya que una vez que el votante ha sido identificado como legítimo para votar, éste emite su voto de manera privada y lo deposita en la urna. Esta separación entre voto e identidad del votante es una tarea compleja en el voto electrónico remoto. Las causas de esta complejidad se explicarán con más detalle en la siguiente sección.

- *Precisión*. El resultado de la elección debe proceder exactamente de los votos emitidos de manera legítima. Es decir, solamente los votos válidos provenientes de votantes legítimos deben ser tomados en cuenta. Por lo tanto, los votos duplicados o no válidos deben ser excluidos del escrutinio. Además, debe prevenirse cualquier alteración de los votos. Cualquier intento de quebrantar la integridad de los resultados de la elección debe ser detectado oportunamente.

- *Equidad*. No se deben conocer resultados parciales durante la fase de votación, de lo contrario dicho conocimiento podría influir en la decisión de los votantes que aún no han emitido su voto.

- *Verificación individual*. En un sistema de voto electrónico remoto, cada votante debería poder verificar:
    - que su voto ha sido recibido correctamente por el servidor de votación (verificación de registro correcto) y,
    - que su voto ha sido incluido correctamente en el escrutinio (verificación de escrutinio correcto).

- *Verificación universal*. Un elemento importante para dar fiabilidad a un sistema de voto electrónico remoto es que este sea públicamente verificable, de tal manera que cualquier participante u observador pueda verificar la integridad de los resultados.

- *Incoercibilidad*. Un votante no debería tener la posibilidad de probar a un tercero la opción o candidato que ha elegido en una elección, ya que el poder probarlo facilitaría la coerción o venta de votos.

- *Robustez*. Un sistema de voto electrónico remoto debería ser tolerante a fallos tecnológicos, así como prevenir ataques de denegación de servicio. Por otro lado, un sistema de voto electrónico remoto debería ser resistente a ataques derivados de confabulaciones de autoridades deshonestas que intenten llevar a cabo una

ataque contra el sistema de votación, por ejemplo violar la privacidad de los votantes o alterar los resultados de la elección.

3.5 Dificultad para proporcionar seguridad a los sistemas de votación

Antes de analizar la dificultad que existe para proporcionar la seguridad requerida a los sistemas de voto electrónico remoto es importante hacer notar que incluso los sistemas de voto convencional, es decir, aquellos basados en papeletas de votación, presentan importantes problemas de seguridad. A continuación se describen algunos ejemplos:

- *Cadena de votos*. Se podría pensar que un ataque de coerción o venta de votos es exclusivo de entornos remotos. Sin embargo, en un sistema de voto convencional se puede presentar un ataque de cadena de votos como el descrito en [Jo05a]. Para llevarlo a cabo, el atacante necesita obtener una papeleta de votación en blanco. Dicha papeleta es marcada con las opciones de voto deseadas por el atacante y la entrega a un votante coaccionado o que desea vender su voto. El votante entra en el recinto de votación ocultando la papeleta. Una vez que un oficial de la elección entrega al votante una papeleta en blanco, el votante accede a la cabina de votación y de manera privada intercambia las papeletas, entonces deposita en la urna la que le fue entregada por el atacante y sale del recinto de votación ocultando la papeleta en blanco. Esta papeleta en blanco será la prueba ante el atacante de que la papeleta depositada en la urna ha sido la encomendada. El atacante tiene entonces una nueva papeleta en blanco, por lo que puede seguir llevando el ataque con el mismo procedimiento tantas veces como personas coaccionadas o vendedoras de su voto tenga disponibles.

- *Prueba del voto*. Además del ataque de coerción descrito en el punto anterior, se puede llevar a cabo un ataque en el que el votante obtenga una prueba de su papeleta marcada. Esto puede lograrse simplemente tomando una fotografía de la papeleta con las opciones marcadas mientras el votante se encuentra en el entorno

privado de la cabina de votación. La fotografía es mostrada al atacante para comprobarle que se ha llevado a cabo su petición. Considerando que en la actualidad resulta muy fácil portar discretamente una cámara fotográfica, por ejemplo la incluida en la mayoría de los teléfonos móviles, este ataque es fácil de llevar a cabo. Este ataque puede ser llevado a cabo igualmente en sistemas de voto electrónico presencial, lo que muestra que un ataque de coerción no es exclusivo de los sistemas de voto remoto.

- *Verificación del voto*. En un entorno de voto presencial, el votante deposita su papeleta en la urna física. A partir de ese momento, el votante debe confiar en que su voto será incluido en el escrutinio ya que no existe la manera de verificarlo. La autoridad de la elección usualmente publica los resultados locales por recinto, sin embargo dicha información no le confirma al votante que su voto ha sido contado, o que no ha sido manipulado antes del escrutinio.

El sistema ideal de voto electrónico remoto debería cumplir con todos los requisitos de seguridad descritos en la sección anterior. La mayoría de estos requisitos pueden cumplirse mediante la combinación de técnicas criptográficas y procedimientos. Sin embargo, debido a la naturaleza de un entorno remoto es difícil cumplir algunos de estos requerimientos sin debilitar el cumplimiento otros, tal como se explica a continuación.

3.5.1 Legitimidad del votante y privacidad

En un contexto de voto electrónico remoto es complicado separar el voto de la identidad del votante ya que la autenticación del votante y la emisión del voto se llevan a cabo a través del mismo canal. Para poder votar, el votante debe poseer las credenciales de votación que le acreditarán como votante legítimo, las cuáles son emitidas por una autoridad de la elección. Estas credenciales, que pueden ser por ejemplo un nombre de usuario y una contraseña, deben ser validadas al iniciar la sesión de voto. Una vez validadas, se permite que el votante emita su voto. En este punto tenemos entonces un

votante autorizado para votar y un voto que corresponde a ese votante. Un proceso de autenticación como este pone en riesgo la privacidad del votante, ya que aunque el voto esté cifrado al momento de llegar al servidor de votación, se puede conservar la relación del voto con el votante y una vez descifrado el voto, se violaría la privacidad del votante. Algunas propuestas han abordado este problema, aunque aún existen dificultades para lograr la privacidad del votante de una manera eficiente. Dichas propuestas se describirán en el capítulo 4.

3.5.2 Verificación del voto contra incoercibilidad

El hecho de que un votante pueda verificar que su voto ha sido incluido en el escrutinio podría significar también que es capaz de probarlo a terceras personas. En ese caso, podría facilitarse la coerción o la venta de votos. Recientemente se han propuesto esquemas en los que el votante tiene la posibilidad de verificar que su voto se ha contado sin que esto represente que puede probarlo a terceras personas. Ejemplos de estos esquemas los podemos encontrar en [Ch04 y NA03]. Dichos esquemas están basados en recibos criptográficos de votación y están enfocados a sistemas de votación en dónde la verificación del voto sólo es necesaria en el aspecto de su inclusión en el escrutinio, es decir, en dónde se asume que el voto ha sido registrado correctamente, por ejemplo en los sistemas de voto electrónico presencial. Sin embargo, en entornos remotos de votación es imprescindible contar con mecanismos que permitan la verificación del registro correcto del voto debido a que los votos son enviados desde un terminal de votación que se encuentra fuera del control y supervisión de la autoridad de la elección y a través de una red telemática pública, lo cuál podría facilitar la manipulación del voto antes de ser registrado en el servidor de votación. Por su parte, esquemas de voto remoto basados en papeletas precifradas como los descritos en [MMP02 y SD04] permiten al votante verificar que su voto se ha registrado correctamente, sin embargo también son propensos a coerción.

Tal como se ha descrito en este capítulo, hay importantes dificultades para lograr que un sistema de voto electrónico remoto sea seguro y confiable. Generalmente en una elección hay muchos intereses de por medio, y por esta razón cualquier escenario de votación presenta riesgos de seguridad, debido principalmente a adversarios que tratarán de obtener una ventaja llevando a cabo algún ataque.

3.6 Seguridad y percepción de seguridad

En un sistema de votación tendríamos que distinguir entre la seguridad que puede ofrecer el sistema y la percepción de seguridad que tienen los votantes acerca de dicho sistema. Tal como lo ha descrito Schneier [Sc08], "la seguridad es una realidad y una sensación al mismo tiempo, y estas no son precisamente lo mismo"

En el caso de voto convencional basado en papel se presentan serios problemas de seguridad tal como hemos analizado previamente. Sin embargo, la mayoría de los votantes de los países democráticos confían en este tipo de sistemas. Esta confianza seguramente se debe a que esa es la forma en cómo han votado siempre. Por otro lado, puede haber un sistema de voto electrónico que sea tecnológicamente seguro, que emplee técnicas criptográficas robustas para proveerlo de seguridad, o incluso que haya sido auditado por expertos antes de su uso, y aún así para muchos votantes dicho sistema podría no ser confiable. Esto se debe principalmente a que el votante promedio no es un experto en las técnicas que se emplean para dar ese nivel de seguridad deseado, por lo que sería incapaz de apreciar el cumplimiento de dicha seguridad.

Existen además otros motivos que pueden generar la desconfianza de los votantes hacia un sistema de votación en particular. Por ejemplo, en Holanda se habían estado utilizando sistemas de voto electrónico para elecciones gubernamentales desde hace algunas décadas. Incluso se llegó a utilizar un sistema de votación por Internet para los votantes residentes en el extranjero. Para las elecciones municipales del 2006, cerca del 99 % de los votos fueron emitidos a través de algún sistema de voto electrónico. Por estas razones,

Holanda había sido considerado un ejemplo de modernización en procesos electorales. Las autoridades electorales, así como los votantes confiaban en la seguridad de los sistemas utilizados. Sin embargo, a raíz de un hecho de sospecha de fraude, un grupo activista en contra del voto electrónico llevó a cabo algunas pruebas de algunos de los terminales de votación utilizados y presentó informes que desvelaban problemas de seguridad que afectaban tanto la integridad de los resultados como la privacidad de los votantes. Estos informes llenaron de desconfianza a la autoridad electoral así como a los votantes, por lo que se decidió suspender toda práctica de voto electrónico en futuras elecciones [Lo08].

El ejemplo anterior ilustra la sensación de seguridad que por muchos años se tenía en los sistemas de voto electrónico utilizados a pesar de los problemas "ocultos" de seguridad que tales equipos poseían. Para una mayor comprensión acerca de los factores que influyen en la percepción de la seguridad puede consultarse [Sc08a].

Otro aspecto que va en detrimento de la percepción de seguridad de los votantes es la falta de mecanismos que permitan verificar la correcta intervención de las diferentes entidades participantes en el sistema de votación, tal como lo destaca Mut en su tesis [Mu06].

Un objetivo importante de un sistema de votación debería ser entonces lograr la seguridad requerida y al mismo tiempo considerar que la mayoría de los votantes deben ser capaces de percibirla y por lo tanto generar la confianza en dicho sistema. La confianza de los votantes en un sistema voto electrónico remoto puede lograrse mediante el uso de mecanismos de verificación individual, en donde ellos puedan verificar personalmente y de una manera sencilla el correcto tratamiento de su voto.

3.7 Amenazas de seguridad en los sistemas de voto remoto

La mayoría de los requisitos de seguridad en los sistemas de voto electrónico son necesarios en parte debido a las diferentes amenazas que se pueden presentar en dichos sistemas. Las amenazas son eventos inesperados que pueden suponer un peligro a uno o más de los elementos de la elección, por ejemplo a votos individuales, al resultado de la elección, etc. Una amenaza puede ser deliberada o accidental (por ejemplo a causa de un error o incluso un evento ambiental o natural). Por su parte, un ataque es la realización de una amenaza.

En todo sistema de información existen tres áreas básicas de seguridad que pueden ser afectadas por un ataque: confidencialidad, integridad y disponibilidad [ISO27002]. Aplicando estas áreas de seguridad a los sistemas de votación, las principales amenazas son aquellas que podrían llegar a comprometer alguno de los siguientes objetivos:

a) privacidad del votante (confidencialidad),
b) precisión de los resultados (integridad) y
c) continuidad hasta completar el proceso de elección (disponibilidad).

3.7.1 Vulnerabilidades en un sistema de votación

Un atacante tratará de explotar alguna vulnerabilidad del sistema de votación a fin de comprometer alguno de los objetivos generales de la elección. A continuación se describen algunos ejemplos de vulnerabilidades en un sistema de voto electrónico remoto:

- *Deficiente sistema de registro de votantes*. El sistema de registro es el medio por el cuál se recaba la información de los votantes para formar un censo electoral. Si dicha recolección de datos es ineficiente, no se puede garantizar la correcta verificación de la legitimidad de los votantes durante la fase de votación. Por

ejemplo, un votante legítimo podría ser erróneamente rechazado para votar por un error en la constitución del censo electoral.

- *Deficiente diseño de los mecanismos criptográficos empleados*. Un aspecto esencial en la seguridad de los sistemas de voto electrónico remoto es la criptografía utilizada. Un diseño inapropiado del mecanismo criptográfico podría causar un riesgo importante a la integridad de la elección. El diseño comprende el protocolo, el algoritmo utilizado, la longitud de las claves, el medio de almacenamiento de las claves privadas, etc.

- *Proceso de autenticación débil*. Un proceso robusto de autenticación aceptará solamente votantes legítimos para emitir un voto. Por el contrario, un esquema de autenticación débil afronta el riesgo de aceptar votantes no legítimos, por lo tanto representa una vulnerabilidad que puede ser aprovechada por un atacante.

- *Control de acceso débil a elementos del sistema de votación*. Los elementos lógicos tales como ficheros, bases de datos, claves de cifrado, etc., así como los elementos físicos como son los servidores, terminales de votación, etc., deben ser protegidos de accesos no autorizados. De lo contrario, un atacante podría hacer un uso indebido de los mismos.

- *Terminales de votación inseguros*. Debido a que en un sistema de voto electrónico remoto los terminales de votación están fuera del control de la autoridad de la elección, existe la posibilidad de que dichos terminales tengan problemas propios de seguridad. Ésta es una de las principales vulnerabilidades de un sistema de voto electrónico remoto y podría ser ampliamente aprovechada por un atacante, por ejemplo insertando algún software malicioso que pretenda conocer el contenido del voto o bien, modificarlo antes de ser emitido.

- *Canales de comunicación inseguros*. Debido a que algunas de las transacciones llevadas a cabo durante el proceso de elección se llevan a cabo a través de una red telemática, un canal de comunicación inseguro representa una vulnerabilidad que puede afectar a los objetivos de la elección.

- *Sistema de logs deficiente*. Un registro deficiente de las transacciones llevadas a cabo durante la elección podría ser un punto de debilidad que no garantiza la detección de manipulaciones en la información. Por lo tanto, si no se cuenta con un registro eficiente de las transacciones existe una probabilidad mayor de ataques sin detección.

- *Procesos deficientes en la verificación de elementos*. Durante la configuración de una elección se deben llevar a cabo algunos procesos de verificación. Estos procesos tienen el propósito de determinar la correcta configuración y operación de los elementos que participarán en la elección. Por lo tanto, un proceso de verificación deficiente podría resultar en una situación de vulnerabilidad.

El diseño de un sistema de voto electrónico remoto debe considerar las posibles vulnerabilidades para tratar de evitar que alguno de los objetivos críticos del proceso de elección se vea afectado. Adicionalmente, se debe considerar que en un entorno de votación pueden existir distintos tipos de atacantes, por ejemplo un votante, un oficial de la elección, un miembro del personal técnico, o bien una persona externa, es decir, aquella que no tiene ningún rol dentro de un proceso de elección.

3.7.2 Catálogo de amenazas

En el 2005, el NIST (The National Institute of Standards and Technology) organizó una conferencia cuyo propósito era reunir los puntos de vista de gente con distintos roles en las elecciones de los Estados Unidos para desarrollar un análisis de amenazas contra los diferentes sistemas de votación. El resultado es un catálogo de amenazas [NIST05] que incluye una descripción de cada una de ellas y explica el escenario en el que se pueden

llevar a cabo. Sin embargo, las amenazas recabadas en dicha base de datos están principalmente orientadas al voto convencional basado en papel y al voto electrónico presencial.

A continuación se presenta un catálogo genérico de amenazas para los sistemas de voto electrónico remoto. Debido a la variedad de sistemas de voto remoto, acotaremos el catálogo presentado al escenario de una elección por Internet, lo cuál puede servir como base para otros sistemas de voto electrónico remoto. Este catálogo pretende ayudar a comprender cuáles son los retos de seguridad que afronta un sistema de voto electrónico remoto. Tal como afirma Jones [Jo05b], "un catálogo de amenazas a los sistemas de votación no es una amenaza". El catálogo se describe a continuación:

- *Suplantación de identidad en el proceso de registro*. Si una elección se lleva a cabo de manera remota, es de suponer que para el registro de votantes también se utilicen medios remotos. Esto conlleva la posibilidad de que una persona intente suplir la identidad de otra para obtener unas credenciales de votantes válidas.

- *Manipulación del censo electoral*. El censo electoral está formado por los datos de los votantes autorizados para participar en la elección. Una manipulación en dicho censo puede provocar que un votante legítimo no sea aceptado en la fase de votación. Por otro lado, si se añaden datos de personas ficticias o sin derecho a voto (por ejemplo debido a la edad) en el censo electoral, se pueden usar esas credenciales que corresponden a datos de votantes no legítimos.

- *Adquirir credenciales de votante*. Antes de la fase de votación, el votante recibe las credenciales de votante que le servirán para autenticarse y poder votar. Un atacante puede apoderarse de las credenciales de un votante para votar en su lugar.

- *Manipulación del software*. El software utilizado en cada una de las fases del proceso de elección puede ser un punto de ataque a fin de manipular los procesos

que soportan. El software puede incluir el sistema de registro, el de configuración de la elección, el de votación, el de consolidación de resultados, etc.

- *Daño del hardware o equipo de red*. El hardware incluye los terminales de votación, por ejemplo los servidores, ordenadores personales, etc. Por su parte, el equipo de red incluye los elementos que forman el o los canales de comunicación que se utilizan en los procesos de la elección. Tanto el hardware como el equipo de red pueden sufrir daños provocados, accidentales o incluso ambientales. Dichos daños pueden ocasionar que la elección no se lleve a cabo con normalidad o incluso que pueda ser interrumpida.

- *Configuración errónea de la elección*. La configuración de la elección establece los parámetros utilizados para que todos los procesos se lleven a cabo tal como han sido planeados. Una configuración errónea, la cuál puede ser provocada o accidental, puede alterar el funcionamiento de los procesos de la elección, incluso modificar el resultado de la elección.

- *Manipulación del voto en el terminal de votación.* En un sistema de voto remoto, el votante utiliza un dispositivo personal para emitir su voto. Dicho dispositivo podría estar expuesto a ataques que tratan de modificar el voto escogido por el votante.

- *Votar más de una vez.* El proceso de autenticación del votante debe prevenir que un votante vote más de una vez en la misma elección. De otro modo, existiría una discrepancia entre el número de votantes que participaron y el número de votos recibidos. Esta situación desde luego ocasionaría un resultado de la elección no legítimo. Existen casos en los que el proceso de elección permite rectificar el voto. En estos casos debe existir un control para que solamente el último voto sea tomado en cuenta.

- *Sustitución de votos.* Los votos son recibidos en un servidor y se almacenan en una base de datos. Esta base de datos puede ser el blanco de ataques que pretendan sustituir votos a fin de alterar el resultado de la elección. Un control de acceso inadecuado a la base de datos puede dar lugar a este tipo de ataques.

- *Adición de votos ilegítimos.* Tal como en el ataque anterior, el propósito de la adición de votos es alterar el resultado legítimo de la elección. Esto se puede lograr accediendo a la base de datos en donde se almacenan los votos.

- *Captura de votos.* Debido a que son transmitidos a través de Internet, los votos podrían ser comprometidos por un atacante que logre acceso a la comunicación. El atacante podría simplemente tratar de conocer el contenido del voto o bien, podría actuar como man-in-the-middle para sustituir el voto durante su transmisión.

- *Fuerza bruta para obtener claves privadas de la elección.* La privacidad de los votos radica en gran parte en la fortaleza del algoritmo de cifrado utilizado y en la protección de la clave privada que se utilizará para descifrar los votos. Por esta razón, la clave privada debe permanecer segura durante la elección. Un adversario podría tratar de obtener la clave privada de la elección mediante un ataque de fuerza bruta. Además de la clave privada para descifrar los votos, pueden existir en el sistema de voto otras claves privadas susceptibles a un ataque de fuerza bruta, por ejemplo las claves utilizadas para firmar digitalmente algunos de los datos.

- *Denegación de servicio.* Evitar que ciertos votantes accedan al sistema de votación puede representar una ventaja para un adversario. Esto se puede dar por medio de un ataque de denegación de servicio (DoS) en el que se inhabilite por ejemplo el servidor de registro, el servidor de votación, etc.

- *Confabulación de la mesa electoral.* Usualmente los miembros de la mesa electoral tienen importantes privilegios de manera compartida y generalmente ellos representan diferentes intereses. Sin embargo, una confabulación maliciosa de dichas personas (aún entre algún subconjunto de ellas) puede alterar el resultado de la elección o violar la privacidad de los votantes.

- *Manipulación de los resultados.* Una vez que los votos han sido consolidados y contabilizados, el resultado podría ser manipulado para beneficiar a cierto candidato.

- *Coerción.* En una elección llevada a cabo a través de un sistema de voto por Internet, tal como en cualquier otro sistema de votación, existe el riesgo de coerción o venta de votos. Un atacante tratará de coaccionar al mayor número de votantes posible a fin de obtener una ventaja considerable.

Cada una de las amenazas descritas en el catálogo puede presentarse en una o más fases de la elección. Estas fases ya han sido descritas en el capítulo 1 de esta tesis y son: preparación de la elección, votación y consolidación de resultados.

La tabla 3.1 resume las amenazas y la forma en que pueden afectar en las diferentes fases de la elección, así como las vulnerabilidades que cada una de esas amenazas puede explotar. Para la implementación de un sistema de voto electrónico remoto se deben considerar estas amenazas y la forma en cómo se pueden llevar a cabo los ataques relacionados, a fin de definir contramedidas que puedan mitigar los ataques o al menos disminuir la posibilidad de que ocurran o de que afecten al proceso de elección.

Tabla 3.1. Catálogo de amenazas en el voto electrónico remoto

Amenaza	**Objetivo**	**Fases de la elección**	**Origen de la amenaza**	**Vulnerabilidades explotadas**
Suplantación de identidad en el proceso de registro	- Integridad - Disponibilidad	- Preparación	- Votante - Oficial - Técnico - Externo	- Deficiente sistema de registro
Manipulación del censo electoral	- Integridad - Disponibilidad	- Preparación - Votación	- Oficial - Técnico - Externo	- Deficiente sistema de registro - Control de acceso débil
Adquirir credenciales de votante	- Integridad - Disponibilidad	- Preparación - Votación	- Votante - Oficial - Técnico - Externo	- Control de acceso débil - Canales de comunicación inseguros - Deficiente sistema de registro
Manipulación del software	- Integridad - Confidencialidad - Disponibilidad	- Preparación - Votación - Consolidación	- Oficial - Técnico - Externo	- Control de acceso débil - Procesos deficientes de verificación
Daño del hardware y equipo de red	- Disponibilidad	- Preparación - Votación - Consolidación	- Oficial - Técnico - Externo	- Control de acceso débil - Procesos deficientes de verificación
Configuración errónea de la elección	- Integridad - Confidencialidad - Disponibilidad	- Preparación	- Oficial - Técnico - Externo	- Control de acceso débil - Procesos deficientes de verificación
Manipulación del voto en el terminal de votación	- Integridad	- Votación	- Externo	- Deficiente diseño del protocolo criptográfico - Terminal de votación inseguro
Votar más de una vez	- Integridad	- Votación	- Votante	- Deficiente sistema de registro - Proceso de autenticación débil
Sustitución de votos	- Integridad	- Votación - Consolidación	- Oficial - Técnico - Externo	- Control de acceso débil - Sistema de logs deficiente - Procesos deficientes de verificación
Adición de votos ilegítimos	- Integridad	- Preparación - Votación - Consolidación	- Oficial - Técnico - Externo	- Control de acceso débil - Sistema de logs deficiente - Procesos deficientes de verificación

Tabla 3.1 (*continuación*). Catálogo de amenazas en el voto electrónico remoto

Amenaza	Objetivo	Fases de la elección	Origen de la amenaza	Vulnerabilidades explotadas
Captura de votos	- Integridad - Confidencialidad	- Votación	- Externo	- Deficiente diseño del protocolo criptográfico - Proceso de autenticación débil - Canal de comunicación inseguro
Fuerza bruta para obtener claves privadas de la elección	- Integridad - Confidencialidad	- Preparación - Votación - Consolidación	- Técnico - Externo	- Deficiente diseño del protocolo criptográfico
Denegación de servicio	- Disponibilidad	- Votación - Consolidación	- Oficial - Técnico - Externo	- Canal de comunicación inseguro
Confabulación de la mesa electoral	- Integridad - Confidencialidad	- Votación - Consolidación	- Oficial	- Deficiente diseño del protocolo criptográfico - Procesos deficientes de verificación
Manipulación de los resultados	- Integridad	- Consolidación	- Oficial - Técnico - Externo	- Deficiente diseño del protocolo criptográfico - Control de acceso débil - Procesos deficientes de verificación - Sistema de logs deficiente
Coerción	- Integridad	- Votación	- Oficial - Técnico - Externo	- Proceso de autenticación débil - Canal de comunicación inseguro

3.8 Comparativa de sistemas de voto remoto

En el 2005, Krimmer and Volkamer [KV05] introdujeron un esquema para comparar las plataformas de voto postal y el voto por Internet usadas en las elecciones alemanas del GI (asociación alemana dedicada a la promoción de ciencias computacionales). Sin embargo,

dicho esquema está enfocado en evaluar proyectos específicos y no incluye un análisis específico de ambas plataformas. En este estudio se compararán los sistemas de voto remoto (incluyendo voto postal) usados en los Estados Unidos usualmente para votantes residentes en el extranjero. El objetivo de la comparación es establecer las ventajas y desventajas de dichos sistemas.

3.8.1 Criterios de evaluación

Como se ha mencionado anteriormente, cada sistema de votación tiene sus propias características y sus correspondientes riesgos de seguridad. Por lo tanto, es importante definir un esquema que facilite la comparación entre los diferentes sistemas. El esquema definido incluye aspectos de seguridad, usabilidad y de implementación de la elección. Los criterios de seguridad considerados en esta comparativa son los requisitos explicados previamente en este capítulo (legitimidad, privacidad, etc.).

Por su parte, la usabilidad comprende los aspectos relacionados con la conveniencia y comodidad de los votantes en su interacción con el sistema de votación. Es importante evaluar estos aspectos ya que la usabilidad puede afectar directamente a la aceptación de un sistema de votación y por lo tanto al nivel de participación en una elección. Dichos criterios se describen a continuación:

- *Prevención de errores*. El sistema de votación debe prevenir errores de votación involuntarios que se podrían presentar durante una sesión de voto, por ejemplo escoger menos o más de las opciones requeridas. Estos errores son comunes en elecciones complejas y que utilizan un sistema de papeletas de votación, por ejemplo elecciones preferenciales con una gran cantidad de candidatos. En este estudio analizaremos cómo los diferentes sistemas de voto remoto pueden prevenir este tipo de errores.

- *Facilidad de uso*. El sistema de votación debería ser fácil de usar para los votantes con capacidad promedio. Es importante que el sistema de votación cumpla con esta característica a fin de evitar marginación de ciertos grupos de votantes.

- *Accesibilidad*. Los votantes con alguna discapacidad física deberían poder emitir su voto sin la necesidad de asistencia de terceras personas ya que esto puede violar su privacidad.

Finalmente, un sistema de votación debería ser fácil de implementar y gestionar a fin de lograr aceptación entre los oficiales de la elección. Por esta razón es importante considerar los siguientes criterios:

- *Factibilidad de puesta en marcha*. El sistema de votación no debería presentar grandes complicaciones para llevar a cabo su configuración y puesta en marcha. La parte de configuración implica el tiempo y la logística para distribuir el material necesario a los votantes.

- *Facilidad de gestión durante la votación*. El sistema de votación debería ser fácilmente administrado durante el período de votación. Esta facilidad de gestión representa el esfuerzo que los oficiales de la elección deben realizar para llevar a cabo el seguimiento de participación, el soporte a los votantes y la resolución de problemas que puedan presentarse.

- *Facilidad de escrutinio*. Este criterio evalúa el esfuerzo (recursos y tiempo) necesario para llevar a cabo el escrutinio de los votos una vez que la elección ha concluido.

3.8.2 Método de evaluación

Ahora que se han definido los criterios de evaluación que se han tenido en cuenta en este estudio, se precisa cómo han sido evaluados dichos criterios. En el caso de los

requerimientos de seguridad se ha utilizado una metodología estándar de estimación y mitigación de riesgos, lo cuál es una forma común para evaluar la seguridad en diferentes sistemas. En el caso de los criterios de usabilidad y administración del sistema se ha empleado una metodología básica de verificación de cumplimiento de los requerimientos.

Al implementar la metodología de estimación y mitigación de riesgos se inició identificando los riesgos relacionados con cada requisito de seguridad para cada sistema de votación. Posteriormente, se llevó a cabo un análisis de mitigación de los riesgos, en el cuál se evaluó el nivel de vulnerabilidad de cada sistema después de considerar los controles de seguridad que cada uno utiliza.

Al llevar a cabo la estimación de riesgos se han considerado como principales vulnerabilidades aquellas que afectan directamente un criterio de seguridad (confidencialidad, integridad o disponibilidad). Entonces, se analizaron las posibles amenazas que podrían explotar esas vulnerabilidades en cada sistema de votación. Finalmente, se describe el riesgo relacionado con cada amenaza, considerando entre otras cosas, los supuestos necesarios para llevar a cabo la amenaza, el esfuerzo requerido para explotarla, la probabilidad de detectar dicha amenaza y la posibilidad de aislar la amenaza para que no afecte a diferentes elementos del sistema. Debido a que los riesgos pueden ser agrupados en base a la vulnerabilidad explotada, dichos riesgos se han evaluado para cada criterio de seguridad y para cada sistema de votación.

Una vez que fueron definidos los riesgos, se identificaron los posibles controles de seguridad (contramedidas) que pueden ser aplicados a cada riesgo a fin de mitigarlo. Además, se ha evaluado la eficiencia de dichos controles de seguridad para determinar en que forma son capaces de detectar y/o mitigar los riesgos.

La tabla 3.2 muestra un ejemplo del método de evaluación de riesgos utilizado. En este ejemplo, son mostrados dos ataques que actúan en dos sistemas de votación diferentes y cuyo objetivo es modificar la intención de voto de un votante.

Tabla 3.2. Ejemplo de estimación y mitigación de riesgos para dos ataques específicos

Ataque	Sistema de votación	Objetivo	Supuestos	Esfuerzo requerido	Probabilidad de detección	Controles de seguridad	Eficiencia de los controles de seguridad	Aceptación del riesgo
Virus	Internet	Modificar votos	Atacante no sabe cuáles terminales de votación se usarán. Terminales de votación interactúan con el sistema de votación usando un applet.	El virus debe ser ampliamente distribuido para lograr su objetivo. El virus debe ser capaz de cambiar las acciones del applet.	Alta (un ataque que pretende largo alcance es fácil de detectar)	Sensores de red antivirus	Mediana (antivirus y sensores de red no pueden tener control total)	Mayor que en el voto postal
Intrusión durante el transporte o almacena-miento de los votos	Postal	Modificar votos	Los votos son trasnportados y almacenados sin medidas estrictas de seguridad (común en servicio postal)	Evadir vigilancia de los votos	Bajo (debido a custodia ineficiente)	Medidas físicas de control de acceso	Baja (es prácticamente imposible proteger el sistema de intrusiones)	Mediano (el actual-mente aceptado)

3.8.3 Resultados del estudio

Los resultados del estudio comparativo se han compilado en las tablas 3.3, 3.4 y 3.5, las cuáles se muestran a continuación. Se ha asignado un valor de satisfacción del requerimiento en cada sistema de votación evaluado. Dicho valor puede ser “bajo”, para un nivel de cumplimiento insuficiente o de no-cumplimiento; “medio”, para un nivel de cumplimiento con ciertos riesgos y “alto” para un nivel de cumplimiento satisfactorio. Junto con la evaluación se añade una explicación de los factores que contribuyen al nivel asignado. La tabla 3.3 muestra la evaluación de los sistemas respecto a los requerimientos de seguridad. En la tabla 3.4 se resume la evaluación de los aspectos de usabilidad y finalmente, en la tabla 3.5 se muestra la evaluación de los aspectos de la gestión de la elección.

Tabla 3.3. Comparativa de requerimientos de seguridad

Factor de comparación	Voto postal	Voto por fax	Voto por correo electrónico	Voto por Internet
Legitimidad	**Medio** Posibilidad de suplantación (sin consentimiento del votante) para enviar voto. Firmas manuscritas son difíciles de validar o no siempre validadas.	**Bajo** Posibilidad de suplantación (sin consentimiento del votante) para enviar voto. Firmas manuscritas son digitalizadas y por lo tanto fáciles de intervenir.	**Bajo** Posibilidad de suplantación (sin consentimiento del votante) para enviar voto. Firmas manuscritas son digitalizadas y por lo tanto fáciles de intervenir.	**Alto** El uso de medios de autenticación fuerte, como certificados digitales, previene la suplantación de votantes (sin consentimiento del votante).
Privacidad	**Medio** Riesgo de acceso a contenidos de votos postales; el acceso puede presentarse durante el transporte o cuando los sobres son abiertos.	**Bajo** Los votos son recibidos sin protección. Los votantes deben firmar declaración de renuncia a su privacidad.	**Bajo** Los votos son recibidos sin protección. Los votantes deben firmar declaración de renuncia a su privacidad.	**Alto** Los votos pueden ser cifrados antes de su transmisión. Procesos criptográficos, como mixing, pueden implementarse para romper relación voto-votante. Votantes pueden proteger su PC contra software malicioso.
Precisión	**Medio** No hay forma de probar que un voto permanece íntegro durante el proceso de elección. Es posible agregar votos ilegítimos sin detección. Votos pueden ser eliminados durante su transporte. Las firmas manuscritas pueden ser verificadas para detectar intentos de fraude masivo.	**Medio** No hay forma de probar que un voto permanece íntegro durante el proceso de elección. Es posible agregar votos ilegítimos sin detección, sin embargo es posible auditar números de fax para detectar intentos de fraude masivo.	**Bajo** No hay forma de probar que un voto permanece íntegro durante el proceso de elección. . Es posible agregar votos ilegítimos sin detección. Direcciones de correo electrónico pueden ser suplantadas. Correos electrónicos pueden ser eliminados durante transmisión.	**Alto** Los votos pueden firmarse digitalmente, lo que previene manipulación sin detección y adición de votos ilegítimos. Recibos de votación ayudan a detectar eliminación de votos. Votantes pueden proteger su PC contra software malicioso.
Equidad	**Medio** Los contenidos de los votos pueden ser accedidos durante su transporte, y por tanto posibles resultados intermedios podrían ser deducidos.	**Bajo** Los contenidos de los votos son siempre accesibles al momento de recibirlos.	**Bajo** Los contenidos de los votos son siempre accesibles al momento de recibirlos.	**Alto** Votos son cifrados antes de su transmisión. Esquemas de secreto compartido protegen la clave de descifrado.
Verificación individual: registro correcto	**Medio** Existen medios para rastrear los votos enviados. Sin embargo, no hay garantía de que el sobre recibido por los oficiales de la elección contiene el voto enviado por el votante.	**Bajo** No hay garantía de que el fax recibido por los oficiales de la elección contiene el voto enviado por el votante.	**Bajo** No hay garantía de que el voto que se almacena o guarda en un sobre es el enviado por el votante.	**Alto** Se pueden implementar procesos de verificación independiente para asegurarse que el voto cifrado es la intención del votante.
Verificación individual: escrutinio preciso	**Medio** El votante puede verificar que su papeleta está presente en el escrutinio a través de algún medio de rastreo. Sin embargo, el votante no puede estar seguro si el contenido de dicha papeleta es realmente el voto emitido.	**Bajo** El votante no tiene ningún medio para verificar que su voto es incluido en el escrutinio.	**Bajo** El votante no tiene ningún medio para verificar que su voto es incluido en el escrutinio.	**Alto** Un recibo de votación permite al votante verificar que su voto ha sido incluido en el escrutinio.

Tabla 3.3 (*continuación*). Comparativa de requerimientos de seguridad

Factor de comparación	Voto postal	Voto por fax	Voto por correo electrónico	Voto por Internet
Verificación universal	**Medio** Se pueden emplear medidas de rastreo de los votos. Esto detectaría manipulaciones en los votos existentes pero no detectaría votos añadidos.	**Bajo** Es difícil verificar la integridad de las transmisiones llevadas a cabo por fax.	**Bajo** Es difícil verificar la integridad de la trasmisión de correos electrónicos.	**Alto** Se pueden implementar medidas de verificación accesibles para cualquier persona. Auditores pueden revisar la aplicación de votación.
Incoercibilidad	**Bajo** El votante puede mostrar su voto a una tercera parte antes de ser enviado, lo cual facilita coerción o venta de votos.	**Bajo** El votante puede mostrar su voto a una tercera parte antes de ser enviado, lo cual facilita coerción o venta de votos.	**Bajo** El votante puede mostrar su voto a una tercera parte antes de ser enviado, lo cual facilita coerción o venta de votos.	**Medio** Si un votante es coaccionado puede volver a enviar su voto si el esquema lo permite. Alternativamente, kioscos de votación ayudar a prevenir coerción o venta de votos.

Tabla 3.4. Comparativa de requerimientos de usabilidad.

Factor de comparación	Voto postal	Voto por fax	Voto por correo electrónico	Voto por Internet
Prevención de errores	**Bajo** Los votantes no son prevenidos de errores involuntarios que pueden invalidar su voto.	**Bajo** Los votantes no son prevenidos de errores involuntarios que pueden invalidar su voto.	**Medio** Errores involuntarios no pueden ser detectados al momento de enviar el voto. Los votos pueden ser revisados por un proceso automático cuando son recibidos. Sin embargo, la corrección implica un intercambio de correos electrónicos entre el votante y algún oficial de la elección.	**Alto** La aplicación de votación puede detectar errores involuntarios y notificarlo al votante cuando este escoge sus opciones. Esto permite que el votante pueda hacer las correcciones necesarias.
Facilidad de uso	**Alto** La mayoría de los votantes están familiarizados con papeletas.	**Medio** La mayoría de los votantes están familiarizados con papeletas, sin embargo muchos no están familiarizados con el envío de Fax.	**Bajo** Los votantes usualmente deben escanear su papeleta y adjuntar el archivo al mensaje de correo electrónico.	**Medio** Los terminales de votación pueden proveer una interfaz de usuario amigable e intuitiva. Sin embargo, no todos los votantes están familiarizados con este tipo de dispositivos.
Accesibilidad	**Bajo** El uso de papeletas representa un problema para votantes con problemas de visión.	**Bajo** El uso de papeletas representa un problema para votantes con problemas de visión.	**Bajo** El uso de papeletas representa un problema para votantes con problemas de visión.	**Alto** El uso de ordenadores personales facilita la interacción con el sistema de votación a las personas con problemas visuales.

Tabla 3.5. Comparativa de requerimientos de implementación y gestión de la elección

Factor de comparación	Voto postal	Voto por fax	Voto por correo electrónico	Voto por Internet
Factibilidad de puesta en marcha	**Bajo** La implementación de una elección requiere períodos largos para asegurar que el material de la elección llega a tiempo a los votantes.	**Medio** El período de distribución de material puede reducirse ya que el material de la elección puede ser enviado a los votantes por fax. Sin embargo, la automatización de este proceso es compleja.	**Alto** El envío de material de la elección a los votantes puede llevarse a cabo por correo electrónico.	**Medio** No es necesario enviar material de la elección a los votantes, excepto si se requiere enviar credenciales para acceder al sistema de votación. El uso de certificados digitales para autenticación evita esto.
Facilidad de gestión durante la votación	**Medio** La gestión de los votos postales es manual.	**Bajo** Los votos recibidos son puestos en sobres para proteger la privacidad.	**Alto** La gestión de los votos recibidos podría ser automatizada.	**Alto** La gestión de los votos recibidos puede ser automatizada. La gestión de las medidas de seguridad podría darle un poco de complejidad.
Facilidad de escrutinio	**Medio** Los votos son manualmente contados, o en su defecto, colocados en un dispositivo que lleva a cabo el escrutinio automático.	**Medio** Los votos son manualmente contados, o en su defecto, colocados en un dispositivo que lleva a cabo el escrutinio automático.	**Alto** El proceso de escrutinio puede ser automatizado. Sin embargo, pueden surgir problemas de formato, por ejemplo, diferentes resoluciones de la imagen escaneada del voto.	**Alto** El escrutinio es completamente automatizado.

El uso de sistemas de voto remoto es necesario para facilitar que los votantes en áreas remotas o residentes en el extranjero puedan ejercer su derecho. El voto postal ha sido la opción preferida de los gobiernos que quieren ofrecer este derecho a dichos votantes. Sin embargo, se han estado explorando sistemas de voto electrónico como alternativa al voto postal.

Existe una desconfianza general hacia los sistemas de voto electrónico remotos, especialmente los que son basados en Internet. Sin embargo, tal como se ha mostrado en este estudio, al comparar los sistemas de voto postal contra los sistemas de voto electrónico remotos, vemos que el voto postal puede tener problemas de seguridad similares e incluso mayores a los de voto por Internet. Lo anterior no significa que los sistemas de voto por Internet estén libres de riesgos de seguridad, sin embargo dichos riesgos se pueden afrontar con distintas técnicas. Por ejemplo, en un ataque de denegación de servicio en una elección por Internet, el votante detecta el ataque y puede reaccionar buscando otro medio para enviar su voto. En cambio, en un ataque en el que se

interceptan los votos postales, el votante no lo detectará. Por lo tanto, este tipo de ataques que intentan evitar que el voto llegue a su destino resultan más eficientes en el voto postal.

Hemos visto también en este estudio que los sistemas de votación basados en fax y en correo electrónico presentan graves problemas de privacidad. Además, la naturaleza de estos canales de transmisión hace más complejo implementar contramedidas de seguridad que puedan mitigar los riesgos que podrían amenazar la integridad de la elección. Por lo tanto, estos sistemas de votación no se pueden considerar como una buena alternativa para el voto por correo postal.

En cuanto a los aspectos de usabilidad e implementación y gestión de la elección, el uso de un sistema de voto por Internet no presenta serias dificultades para cumplir con los criterios evaluados. De hecho, podemos ver cómo en ambos casos presenta algunas ventajas respecto al voto postal. Por ejemplo, un sistema de voto por Internet puede prevenir errores involuntarios del votante durante la sesión de voto e incrementa la accesibilidad para votantes con problemas visuales. Además, proporciona elementos adicionales que facilitan la auditoria.

3.9 Propuesta de transición hacia el voto remoto por Internet

El uso de Internet en los sistemas de votación supone una ventaja para eliminar restricciones espaciales a los votantes, y por lo tanto facilitan su movilidad. Sin embargo, el espacio público que Internet representa constituye su principal debilidad por los riesgos de seguridad que eso implica. Por esta razón es complejo llevar a cabo una elección por Internet sin poner en riesgo su integridad. De todos modos, existen importantes avances que se han visto motivados por las ventajas que ofrece un sistema de voto por Internet, tal como se ha descrito en el capítulo 1 de ésta tesis.

Por otro lado, existen tendencias que refutan la factibilidad de un proceso de votación llevado a cabo a través de Internet. Se argumenta el problema de la brecha digital, en el cuál sólo una minoría de ciudadanos tiene acceso a Internet y a otros recursos tecnológicos. Además, se tiene el temor de que con el voto por Internet surjan nuevos tipos de fraude. Al respecto, la "California Internet Voting Task Force" [Ca00] sugirió una evolución gradual hacia el voto remoto por Internet para elecciones gubernamentales basada en cuatro etapas. En la primera y segunda etapas, el proceso de votación debería llevarse a cabo en recintos de elección bajo la supervisión de oficiales de la elección. En la tercera etapa, el votante puede enviar su voto a través de recintos o kioscos sin supervisión de oficiales de la elección. En la cuarta etapa el voto puede llevarse a cabo desde cualquier ordenador conectado a Internet.

La brecha digital se ha reducido considerablemente en los últimos años, ya que el uso de Internet se ha incrementado entre todo tipo de personas. Esto hace posible una adaptación más fácil del voto remoto desde un punto de vista social. Además, la mejora en las infraestructuras de telecomunicaciones y en los algoritmos y protocolos criptográficos permite asegurar en un nivel alto la privacidad e integridad de los votos. De manera adicional, existen nuevas técnicas de autenticación basadas en sistemas biométricos y dispositivos de almacenamiento protegidos como las tarjetas inteligentes. A modo de ejemplo, se puede resaltar la experiencia española con la implementación del DNI electrónico, que facilita la gestión de diversos trámites y servicios gubernamentales. Por estas razones, podemos considerar que es posible introducir un sistema de voto electrónico remoto de una forma menos gradual que la propuesta en [Ca00]. Actualmente algunos países hacen uso del voto postal para permitir votar a los votantes que no pueden acudir a un recinto electoral el día de la votación. Considerando la comparativa de sistemas de voto remoto llevada a cabo en la sección anterior, el voto por Internet es adecuado para reemplazar al voto postal.

En esta sección se propone un esquema que contempla el voto por Internet en distintos escenarios de manera simultánea, tal como será descrito a continuación.

3.9.1 Presentación del esquema

A continuación se describirán los elementos del esquema, los participantes y el funcionamiento del protocolo a lo largo del proceso de votación.

Tarjeta de votación para la autenticación del votante

En el esquema se hace uso de una tarjeta de votación basada en una tarjeta inteligente en red (network smart card). Las propiedades de esta tarjeta permiten llevar a cabo una autenticación robusta del votante. El votante se autentifica frente a la autoridad electoral (de manera presencial o remotamente) por medio de este dispositivo. También permite llevar a cabo la autenticación frente al sistema de votación. Además, es utilizada para cifrar y firmar digitalmente el voto escogido.

Una tarjeta inteligente en red contiene las mismas características físicas y lógicas que una tarjeta inteligente convencional, es decir, es un dispositivo dónde se almacena información crítica de manera segura [VW98]. Algunos autores como Urien [Ur00] y Montgomery y otros [MAL04] propusieron integrar las tarjetas inteligentes con la pila del protocolo TCP/IP para simplificar la interconexión de la tarjeta con los ordenadores personales. Esto permite el uso de la tarjeta para aplicaciones basadas en Internet sin la necesidad de software o dispositivos adicionales. Éste es el principio fundamental de una tarjeta inteligente en red. Además cuenta con propiedades de comunicación de datos, portabilidad, creación de firmas digitales, así como capacidad de procesamiento. Su seguridad lógica también depende del uso del PIN (personal identification number). La tarjeta inteligente en red puede establecer una comunicación segura con un servidor remoto por ejemplo a través de TLS. De hecho, este tipo de tarjeta es definida como un nodo seguro de Internet [MAL04].

De manera complementaria, y para que la autenticación sea aún más robusta, en este esquema se hace uso de la huella dactilar del votante. De esta manera, se previene el uso

de la tarjeta de votación por parte de una persona no autorizada, reduciendo al mismo tiempo la posibilidad de coerción o venta de votos.

Para llevar a cabo estas tareas, la tarjeta de votación debe ser configurada inicialmente con los siguientes datos:

impresos:

- Datos personales del votante (nombre, dirección, número de distrito o colegio electoral, etc.).
- Fotografía del votante.

y almacenados:

- Certificado digital del votante.
- Clave pública de la autoridad de autenticación.
- Clave pública de la autoridad de escrutinio.
- Clave pública de la autoridad receptora del voto.

La misma tarjeta de votación puede extender su uso a otras actividades gubernamentales o de negocios a fin de aprovechar sus recursos.

Participantes del esquema

En la figura 3.2 se muestran los participantes necesarios para el esquema. Estos son definidos a continuación:

- Votantes. Todos los ciudadanos autorizados para ejercer su derecho al voto. Usualmente, estos son previamente registrados para constituir una base de datos de votantes legítimos (censo electoral). A los votantes se les debe entregar una tarjeta de votación, la cuál les permitirá autenticarse y emitir su voto.

- Autoridad de la elección. Esta entidad es la responsable para preparar la elección, dar a conocer la lista de candidatos, etc. Además está a cargo de supervisar y validar todo el proceso de la elección.

- Autoridad de registro. Esta entidad está encargada de mantener actualizada la lista de votantes legítimos. También se encarga de proveer las tarjetas de votación a los votantes y de administrar los certificados digitales de los mismos.

- Autoridad de autenticación. Durante la fase de votación, esta autoridad verifica la identidad de los votantes y determina su legitimidad. La autoridad de autenticación debe ser constituida por dos o más entidades con la finalidad de cubrir los diferentes escenarios del esquema, los cuáles serán descritos más adelante.

- Autoridad de votación. Esta entidad es la que se encarga de recibir los votos cifrados y de mantenerlos protegidos hasta el final de la fase de votación, cuando dichos votos serán transferidos a la autoridad de escrutinio.

- Autoridad de escrutinio. Es la autoridad a cargo del descifrado y escrutinio de los votos, así como de publicar los resultados. Esta autoridad está constituida por diferentes entidades que comparten la clave privada de la elección, la cuál es utilizada para el descifrado de los votos.

Las autoridades de autenticación, de votación y de escrutinio están a cargo de servidores que permiten llevar a cabo las tareas que les corresponden. Dichos servidores los llamaremos servidor de autenticación, servidor de votación y servidor de escrutinio, respectivamente. Debido a que los dos primeros servidores deben estar conectados a Internet, es recomendable que se mantengan servidores de redundancia para prevenir que fallos o ataques de denegación de servicio interrumpan los procesos de la elección.

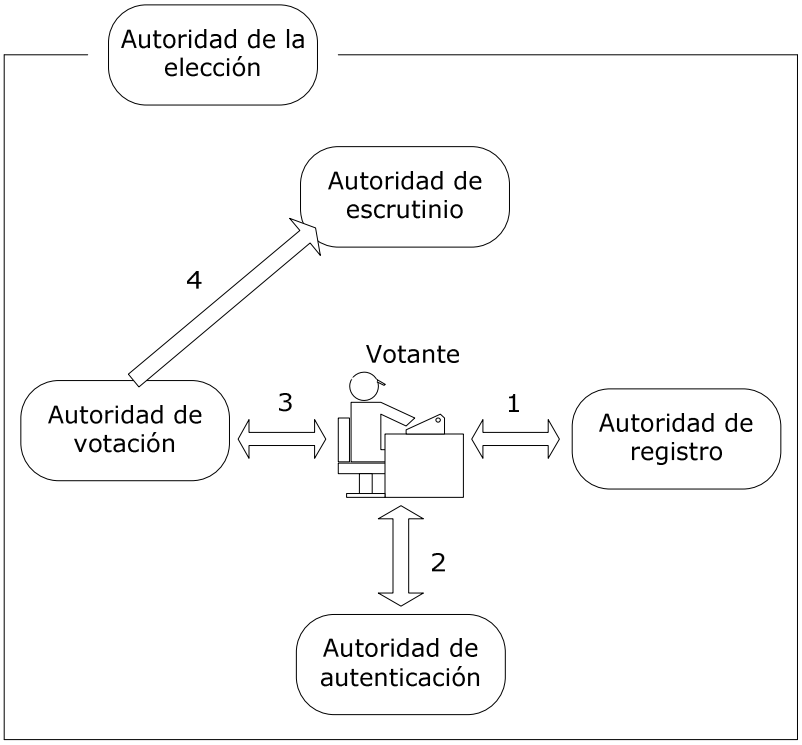

Figura 3.2. Participantes y su interacción en el esquema propuesto

3.9.2 Desarrollo del protocolo durante las fases de la elección

El esquema propuesto está definido para actuar en un proceso completo de una elección. Dicho proceso abarca las 3 fases de la elección descritas en el capítulo 1: preparación, votación y consolidación de resultados. En esta sección se describen los procedimientos llevados a cabo por el esquema en las diferentes fases. La nomenclatura utilizada en los procesos que se explican a continuación se muestra en la tabla 3.6.

Fase de preparación

- Anuncio de la elección. La autoridad de la elección publica el propósito de la elección, la fecha, lista de candidatos, Etc.

- Registro de votantes (relación 1 en la figura 3.2). El proceso de registro se lleva a cabo para recabar la información de los votantes tal como su información personal y su huella dactilar. Las plantillas de las huellas dactilares son almacenadas en un repositorio. Por otro lado, se configuran los parámetros que serán usados para la autenticación remota de cada votante y para la emisión del voto. Estos parámetros son entonces almacenados en la tarjeta de votación. Se asume la existencia de una PKI (Public Key Infrastructure) para la gestión de los certificados digitales. Una vez recabada y configurada dicha información, la autoridad de registro proporciona a cada votante su tarjeta de votación personalizada con sus datos. Al final de este proceso se tendrán los elementos necesarios para llevar a cabo la autenticación de los votantes.

Tabla 3.6. Nomenclatura utilizada en el protocolo de votación

Símbolo	**Descripción**
V	Votante
V	Voto
T	Tarjeta de votación
PIN	Contraseña para desbloquear el acceso a la tarjeta de votación
SA	Servidor de autenticación
SE	Servidor de escrutinio
SV	Servidor de votación
Acc	Solicitud de acceso
Aut	Solicitud de autenticación
$Cert_V$	Certificado digital de votante
$Cert_{SA}$	Certificado digital de servidor de autenticación
$S_{V:SA}$	Clave privada pactada entre votante y servidor de autenticación
P	Clave pública
S	Clave privada
R	Valor aleatorio generado en la tarjeta de votación
C	Factor de cegado generado en la tarjeta de votación
v-Id	Identificador del voto
T-Id	Identificador de tarjeta de votación
T-Id'	Identificador de tarjeta de votación, almacenado en *SA*
H	Plantilla de huella dactilar de votante
H'	Plantilla de huella dactilar de votante, almacenada en *SA*
Seq	Número secuencial

Fase de votación

- Autenticación presencial (relación 2 en la figura 3.2). El votante es autenticado para poder emitir su voto. Esto se lleva a cabo a través de la autoridad de autenticación quien autoriza el acceso al sistema de votación una vez que la tarjeta de votación que posee el votante ha sido validada. Este paso se lleva a cabo solamente en escenarios de voto bajo supervisión. Dichos escenarios son descritos en la sección 3.9.3.

- Establecimiento de sesión. Para llevar a cabo un establecimiento de sesión se hace uso de la tarjeta de votación, la cuál permite por un lado identificar que la persona que la porta es un votante legítimo y por otro lado verificar los datos del votante en el servidor de autenticación. El proceso es el siguiente:

    1. El votante V_i conecta su tarjeta de votación T_i a un ordenador. Entonces se solicita al votante que teclee su *PIN*.

    2. El sistema de control de acceso de la tarjeta de votación compara el *PIN* que se ha tecleado con el *PIN* almacenado en la tarjeta de votación. Si ambos *PIN* concuerdan, entonces se permite al votante V_i utilizar su certificado digital y su par de claves.

  Después de esta verificación local, la tarjeta de votación T_i se puede conectar remotamente al servidor de la autoridad de autenticación *SA*. Esto es posible ya que T_i conoce la URL del servidor [LA04]. La comunicación de datos entre la tarjeta de votación y dicho servidor de autenticación remota se lleva a cabo de una manera segura a través del protocolo TLS. En la figura 3.3 se muestra el intercambio de mensajes entre el servidor de autenticación y la tarjeta de votación a fin de establecer un identificador de sesión. Dicho proceso se explica a

continuación:

1. La tarjeta de votación T_i envía un mensaje de solicitud de acceso *Acc* al servidor de autenticación *SA*.

2. *SA* envía su certificado digital $Cert_{SA}$ a T_i.

3. T_i envía el certificado digital del votante $Cert_{vi}$ al servidor *SA*.

4. *SA* verifica la autenticidad del $Cert_{vi}$ y genera una clave secreta $S_{V:SA}$.

5. *SA* envía un mensaje $((S_{V:SA})_{S\text{-}SA})_{P\text{-}V}$ a T_i.

6. T_i almacena la clave simétrica $S_{V:SA}$.

7. T_i genera un valor aleatorio *r* y lo cifra con la clave previamente generada. Posteriormente envía el mensaje $(r)S_{V:SA}$ al servidor *SA*.

8. *SA* descifra $(r)S_{V:SA}$ y almacena *r* para una futura autenticación.

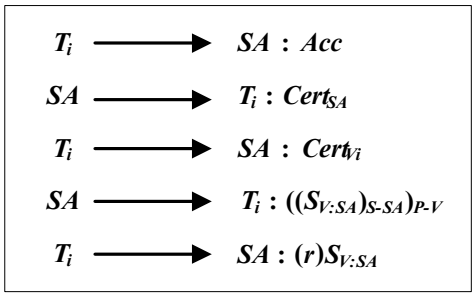

Figura 3.3. Establecimiento de un identificador de sesión

- Selección de candidatos. Una vez que el votante ha sido autenticado, se le permite acceder a la plataforma de votación y se le muestran las opciones o candidatos. Entonces el votante escoge sus preferencias de voto.

- Autenticación remota. El votante V_i continúa con el proceso de votación llevando a cabo los siguientes pasos:

    1. V_i envía un mensaje *Acc* al servidor *SA*.

    2. *SA* envía un mensaje de solicitud de autenticación *Aut* a V_i.

    3. A través del lector de huella dactilar se obtiene la plantilla de la huella dactilar h_i de V_i.

    4. El lector de huellas envía h_i a T_i.

    5. T_i cifra el voto v_i con la clave pública de la autoridad de escrutinio y calcula un factor ciego c_i del voto cifrado:$((v_i)_{P\text{-}SE})$ (c_i)

    6. T_i genera un número aleatorio de identificación del voto $v\text{-}Id_i$.

    7. T_i envía el voto al servidor de autenticación *SA*. Junto con el voto se añaden el identificador de la tarjeta de votación $T\text{-}Id_i$ y el identificador del voto $v\text{-}Id_i$:

    $$(r, h_i, T\text{-}Id_i, v\text{-}Id_i, ((v_i)_{P\text{-}SE})(c_i))S_{V:SA}$$

    8. *SA* lleva a cabo la verificación de la tarjeta de votación. Si $T\text{-}Id_i = T\text{-}Id_i$', se continúa con el siguiente paso, en caso contrario el proceso finaliza.

    9. *SA* verifica que $h_i = h_i$'. h_i debería coincidir con el h_i' almacenado y asociado al T_i correspondiente.

    10. *SA* asigna y añade al voto un número secuencial Seq_j (empezando con 1 e incrementando el valor secuencialmente si el mismo votante envía otro

voto durante el proceso de votación).

11. *SA* elimina del mensaje los valores h_i y $T\text{-}Id_i$.

12. *SA* envía a T_i el mensaje verificado y firmado digitalmente:

$$(v\text{-}Id_i, Seq_j, ((v_i)_{P\text{-}SE})(c_i))_{S\text{-}SA}$$

Este protocolo de autenticación se muestra en la figura 3.4.

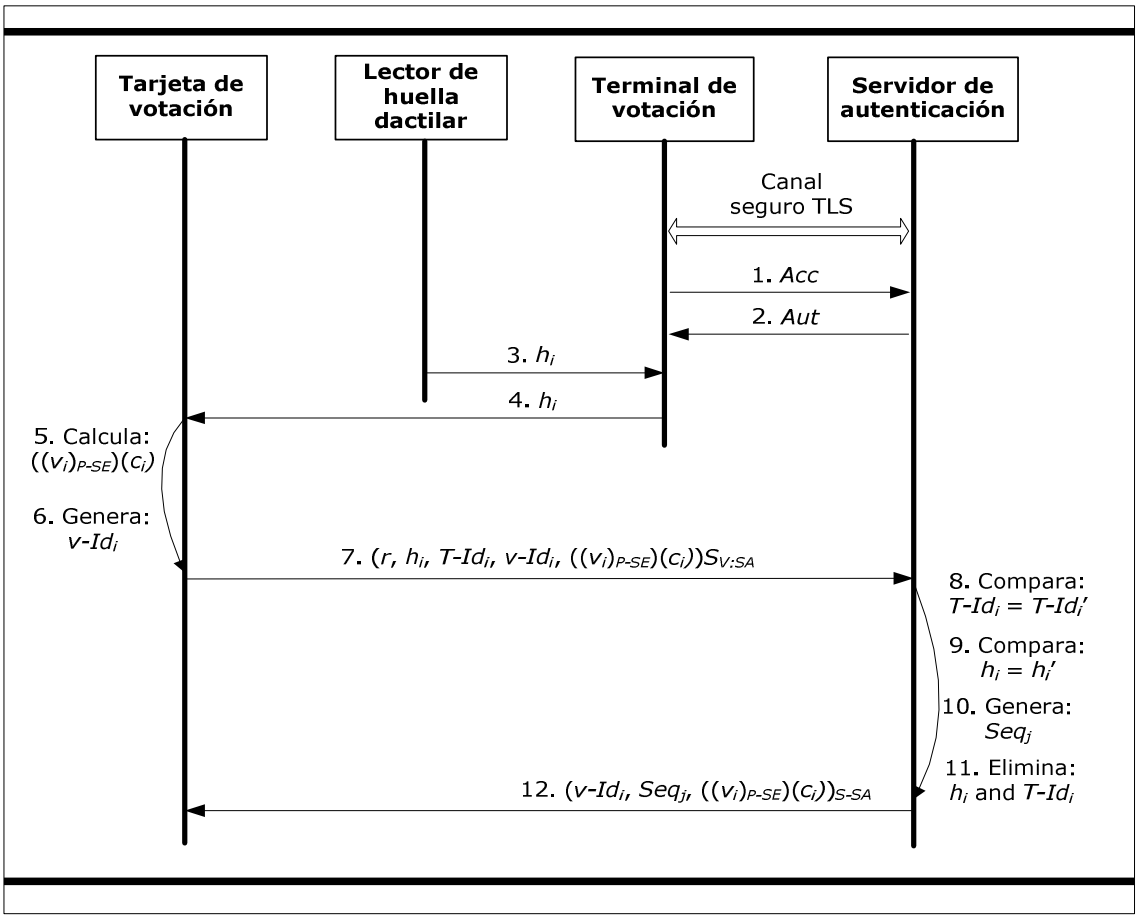

Figura 3.4. Protocolo de autenticación remota

- Envío del voto. Después de que el proceso de autenticación remota se ha llevado a cabo con éxito, la tarjeta de votación contiene el mensaje del voto validado y firmado digitalmente por la autoridad de autenticación.

1. El voto es desvelado por la tarjeta de votación:

$$((v\text{-}Id_i, Seq_j, ((v_i)_{P\text{-}SE})(c_i))_{S\text{-}SA}) \,/\, c_i$$

2. El votante envía el mensaje conteniendo el voto a la autoridad de votación:

$$((v\text{-}Id_i, Seq_j, (v_i)_{P\text{-}SE})_{S\text{-}SA})$$

La transmisión del voto se lleva a cabo a través de una conexión TLS de autenticación simple. Esto es porque la tarjeta de votación desea saber que está conectada al servidor correcto pero el servidor no debería saber quién está solicitando la conexión a fin de proteger la privacidad del votante. Por otro lado, para prevenir ataques de denegación de servicio (DoS), la única forma de conectarse al servidor de la autoridad receptora es siendo redirigido desde el servidor de autenticación. De esta forma, sólo los votantes previamente autenticados pueden establecer una conexión con el servidor de votación.

- Validación de los votos. Al terminar la fase de votación, la autoridad de votación lleva a cabo una validación de los votos recibidos. Esta validación consiste en verificar si hay más de un voto con el mismo *T-Id*, en cuyo caso, sólo el voto que tenga el número secuencial más alto será incluido en el escrutinio. Esto es para evitar que se considere en el escrutinio más de un voto proveniente del mismo votante.

Consolidación de resultados

- Transferencia de los votos (relación 4 en la figura 3.2). Al final de la fase de votación, la autoridad de votación transfiere los votos, de una manera segura, a la autoridad de escrutinio.

- Permutación de los votos. Una función de permutación es usada para cambiar el orden original de los votos a fin de romper cualquier relación de los votos con los votantes, asegurando de esta manera la privacidad.

- Descifrado y escrutinio. Los votos son descifrados mediante un esquema de secreto compartido, en donde la clave privada *S-SE* es compartida entre un conjunto predefinido de personas que componen la autoridad de escrutinio. De esta manera se le da mayor seguridad al proceso de descifrado y escrutinio. El proceso entonces puede ser compartido entre *n* personas a través de un sistema umbral de cifrado de clave pública (t, n) como en [IS90 y Pe91]. Cada uno de las entidades de escrutinio tiene una parte de la clave privada. Entonces, para el descifrado se requiere un subconjunto de *t* personas, cada una de ellas cooperando con su parte de la clave.

- Publicación. La autoridad de escrutinio, bajo la supervisión de la autoridad de la elección, publica el resultado final de la elección.

3.9.3 Escenarios de votación

Tal como se ha mencionado previamente, la propuesta contempla un esquema de votación multi-canal. Este esquema consiste de cuatro escenarios trabajando simultáneamente, de esta manera se puede cubrir todo tipo de votantes. Los escenarios son los siguientes:

Escenario 1: Votación convencional en un recinto asignado.

El último día programado para recibir votos son abiertos los precintos de votación. Estos recintos son los tradicionales y ya conocidos por los votantes, en los cuáles hay oficiales de la elección supervisando el procedimiento de votación. Los votantes sin experiencia

en el uso de ordenadores pueden acudir al recinto de votación que les corresponde para emitir su voto a la manera tradicional.

El votante debe mostrar su tarjeta de votación a los oficiales que están a cargo del precinto. Los oficiales consultan el censo electoral para comprobar la legitimidad del votante así como si a dicho votante le corresponde votar en ese recinto. Entonces se incluye una marca en el censo electoral que indica que el votante ha emitido su voto por medio de este escenario. De esta manera, ningún votante que haya votado a través del esquema tradicional puede volver a votar, ni por el mismo escenario ni por uno diferente. Una vez autenticado, el votante marca sus opciones en una papeleta y posteriormente la coloca en una urna física. Al final de la elección, el escrutinio de estos votos se lleva a cabo también de la manera convencional.

Escenario 2: Votación electrónica desde cualquier recinto.

Los votantes que tengan alguna experiencia con el uso de ordenadores pueden votar a través de este escenario. En este, el votante puede acudir a votar a cualquier recinto supervisado. Al igual que en el escenario anterior, el votante es autenticado mostrando su tarjeta de votación. La fase de establecimiento de sesión se lleva a cabo bajo supervisión y una vez que se comprueba la legitimidad del votante se abre una sesión de voto en alguno de los terminales de votación disponibles. El votante escoge y confirma sus opciones de votación, entonces se llevan a cabo la autenticación remota y el proceso de votación tal cómo se ha explicado en el protocolo de votación.

Debido a que los escenarios 1 y 2 tienen en común un entorno de votación supervisado, definimos a continuación la preparación que los precintos deben tener. Todos los recintos de votación deben ser considerados tanto para votación convencional así como electrónica. Por lo tanto, deben contar con los siguientes elementos:

- Un ordenador principal para la fase de login.
- Papeletas y urnas convencionales.

- Terminales de votación para votación electrónica por Internet provistos de lectores de huella dactilar.

Escenario 3: Votación electrónica por Internet desde recintos sin asistencia.

Los votantes que deseen emitir su voto sin asistencia pueden hacerlo en recintos habilitados para ello. Los terminales de votación instalados en dichos recintos deben contar con una conexión a Internet, así como lectores para la tarjeta de votación y para la huella dactilar. De esa manera, se puede llevar a cabo la autenticación del votante sin necesidad de supervisión, ya que solo podrán ser considerados votantes legítimos aquellos que porten su tarjeta de votación. El proceso completo de autenticación y votación se lleva a cabo como se ha explicado en el protocolo de votación.

Escenario 4: Votación electrónica por Internet desde cualquier lugar.

Los votantes que cuenten con los medios tecnológicos para enviar su voto desde una conexión a Internet particular pueden hacerlo bajo este escenario. Para esto, es necesario tener lectores de huella dactilar y de tarjeta de votación, tal como los terminales de votación del escenario 3. El proceso de votación se lleva a cabo tal como se ha descrito el protocolo.

Múltiple voto

El esquema permite llevar a cabo la práctica de múltiple voto, es decir, que un votante legítimo puede votar más de una vez. El propósito es disminuir los ataques de coerción y venta de votos. Una manera que tiene el atacante de comprobar que el votante ha votado en cierto sentido es hacer que el votante envíe su voto en presencia del atacante. En este esquema, el votante puede cambiar su voto en cualquier momento enviando un nuevo voto. Cada vez que un nuevo voto es recibido en el servidor de votación, este será el voto válido para ese votante, por lo tanto el o los votos anteriores no serán considerados en el escrutinio. La validación de un solo voto por votante es gestionada de acuerdo a lo descrito en el protocolo de votación.

La única restricción para aceptar un nuevo voto es cuando el votante ha votado previamente en papel. En este caso no es posible emitir un nuevo voto, sin embargo no sería necesario ya que esta opción se tuvo que haber dado bajo supervisión por lo que se descarta un ataque de coerción.

Llevando a cabo la opción de múltiple voto, la única opción para un ataque de coerción exitoso consiste en que el atacante permanezca con el votante durante todo el período de votación, lo cuál no es factible para un atacante. Otra opción es que el atacante esté con el votante hacia el final del período de votación y el voto se lleve a cabo en ese momento, para así asegurarse que no habrá un voto después de ese. En este caso, se requeriría un atacante por cada votante, lo cuál tampoco es factible para un ataque que pretenda cambiar los resultados de una elección.

3.9.4 Análisis de Seguridad

Los sistemas de votación por Internet son vulnerables a diferentes ataques. A continuación se describen los posibles ataques contra el esquema propuesto y cómo estos pueden ser mitigados.

Robo de la tarjeta de votación. La intención de este ataque es usurpar la identidad de un votante durante la elección. Este ataque no es factible ya que para lograr una autenticación válida se requiere, además de la tarjeta de votación, la huella dactilar del votante.

Compra de tarjeta de votación. Al igual que en el ataque anterior, el propósito es usurpar la identidad de un votante legítimo. Este ataque sería solamente efectivo si el votante además de vender su tarjeta de votación, coopera con su huella dactilar. Debido a esta restricción, es improbable un ataque masivo de este tipo.

Manipular una tarjeta de votación. Existen ataques que podrían tratar de manipular u obtener información almacenada en la tarjeta de votación. En el esquema presentado, un ataque como el descrito no afectaría seriamente la integridad de la elección. La información comprometida sería básicamente la clave privada del votante. Sin embargo, esta clave no sería suficiente para emitir un voto haciéndose pasar por el votante legítimo, ya que la plantilla de la huella dactilar no se encuentra en la tarjeta de votación.

Captura de la huella dactilar. Algún tipo de software malicioso podría capturar la plantilla de la huella dactilar cuando esta es enviada desde el lector de la huella hacia la tarjeta de votación. Sin embargo, este ataque no representa un riesgo si el atacante no posee la tarjeta de votación.

Además de mitigar los ataques previamente descritos, el esquema de votación propuesto satisface los requerimientos básicos de un sistema electrónico de votación y de manera especial logra que los votantes puedan verificar la inclusión de su voto en el escrutinio. A continuación se describe cómo se satisfacen esos requerimientos:

Legitimidad. Por medio del protocolo de autenticación definido en el esquema, se puede asegurar que solo los votantes legítimos pueden votar. Este esquema requiere tres parámetros para autenticar a un votante: algo que se es, algo que se posee y algo que se conoce, además de un identificador de sesión. Si uno de estos parámetros es incorrecto, entonces no es posible aceptar a un votante como legítimo. La usurpación de identidad se podría llevar a cabo exitosamente solo mediante la colaboración total del votante, lo cuál realmente no sería usurpación de la identidad.

Privacidad. La división del dominio de autoridad ayuda a preservar la privacidad del votante. Mientras que la autenticación es llevada a cabo ante un servidor de autenticación a cargo de una autoridad, el voto cifrado es recibido por una autoridad diferente a fin de prevenir alguna relación entre votos y votantes. Por otro lado, la función de permutación que se aplica a los votos antes de su descifrado evita que se relacionen los votos con los votantes.

Precisión. Solo los votos válidos forman parte del escrutinio. Cuando un segundo o tercer voto es recibido, el anterior es siempre descartado.

Equidad. Los votos cifrados son preservados por la autoridad a cargo del servidor de votación hasta el final de la fase de votación y solo la autoridad de escrutinio posee la clave de descifrado. De esta manera, nadie puede conocer resultados parciales de una elección.

Verificación. Cualquier observador puede verificar que las listas publicadas concuerdan con los resultados de la elección.

Incoercibilidad. Debido a los parámetros de seguridad de la tarjeta de votación y al uso de la huella dactilar, se previene el uso de la tarjeta por una persona ilegítima. Esto reduce la posibilidad de coerción y venta de votos. Por su parte, la posibilidad del múltiple voto también contribuye a reducir las posibilidades de coerción debido a que los atacantes no podrían estar seguros si el votante ha enviado otro voto después del voto comprometido.

Robustez. El esquema previene ataques de conspiración de autoridades. Esto se logra debido a que:

a) El voto está cegado cuando lo recibe la autoridad de autenticación, por lo que esta autoridad no sabe nada acerca de la opción elegida por el votante.
b) El voto se encuentra cifrado cuando lo recibe la autoridad de votación, por lo que no tiene conocimiento del contenido del voto. Esta autoridad tampoco conoce la identidad del votante.

   En base a las sentencias a y b, las autoridades de autenticación y de votación no pueden conspirar debido a que el votante tiene un parámetro de sesión diferente con cada uno de estas autoridades.

c) La única autoridad que posee la clave de descifrado es la autoridad de escrutinio, y esta autoridad se encuentra constituida por un conjunto de entidades que comparten dicha clave.

El esquema también contempla la protección contra ataques de denegación de servicio a través del uso de un conjunto de servidores disponibles que constituyen por una parte la autoridad de autenticación, y por otra parte, la autoridad receptora de los votos.

3.10 Conclusiones y aportación

En este capítulo se han presentado los diferentes sistemas de voto remoto, incluyendo el voto postal, el cuál es actualmente el más ampliamente utilizado. Se ha llevado a cabo una comparativa entre dicho sistema y los diferentes sistemas de voto electrónico remoto a fin de evaluar las ventajas que proporcionaría el uso de un sistema de voto electrónico en comparación con el actual sistema de voto postal. Se puede concluir que entre los sistemas de voto electrónico remoto, el voto por Internet es el más adecuado para sustituir al voto postal, debido principalmente a ciertas ventajas de seguridad como son: mayor facilidad para la autenticación del votante, garantía de equidad para los votantes, precisión en el escrutinio y verificación del correcto tratamiento de los votos, etc. Además, sobresalen las características de usabilidad del voto por Internet, como la prevención de errores involuntarios al seleccionar el voto o la facilidad que se ofrece a los votantes con alguna discapacidad visual para llevar a cabo la selección y envío de su voto sin asistencia de terceros. En la sección 3.8 se mostró una comparativa de diferentes sistemas de voto remoto. Esta comparativa de sistemas de votación fue presentada en Bochum, Alemania en la conferencia “E-Voting and Identity” y publicada en [PM07b].

En este capítulo también se ha llevado a cabo un estudio de las vulnerabilidades y amenazas de los sistemas de voto electrónico remoto, de manera más específica, en el voto por Internet. El conjunto de vulnerabilidades y el catálogo de amenazas presentados

en las secciones 3.7.1 y 3.7.2 respectivamente, es parte de un análisis de seguridad llevado a cabo para un proyecto piloto que se realizó para las elecciones presidenciales de los Estados Unidos en Noviembre del 2008. En dicho piloto, militares pertenecientes al condado de Okaloosa, Florida, que residen en tres bases militares ubicadas en el Reino Unido, Alemania y Japón utilizaron un sistema de voto por Internet desarrollado por la empresa Scytl. El resultado de dicho análisis es parte de un informe técnico de Scytl [Sc08b].

En la sección 3.9 se ha descrito un esquema de votación que pretende ser la base para una transición hacia el voto remoto por Internet. El esquema ha sido publicado en el IJEG (International Journal of Electronic Governance). Véase [MSM+08] para los detalles de la publicación. Considerando los elementos que se utilizan en este esquema, como son la tarjeta de votación, y la posibilidad de diversos canales simultáneos de votación, se contribuye a la evolución hacia el uso extensivo del voto electrónico remoto. La tarjeta de votación, la cuál está basada en una tarjeta inteligente en red, junto con el requerimiento de la huella dactilar del votante permite llevar a cabo una autenticación robusta de votantes. El esquema reduce en gran manera la posibilidad de coerción o venta de votos. Primeramente, debido a la baja probabilidad de usurpación de la identidad durante la sesión de voto. Por otro lado, la posibilidad de múltiple voto también contribuye a disminuir la coerción, ya que el votante tiene la posibilidad de enviar un nuevo voto si ha sido coaccionado. En una línea futura de investigación se pretende definir una función de permutación que permita proteger la privacidad de los votantes, al mismo tiempo que se comprueba que dicha función se lleva a cabo de manera honesta.

Capítulo 4

Esquemas Criptográficos de Voto Electrónico Remoto

4.1 Introducción

Los esquemas de voto electrónico remoto pueden clasificarse en 4 grupos. Estos se diferencian en la forma en cómo se utiliza la criptografía para tratar de satisfacer los requisitos de seguridad que se contemplan en una elección. Estos grupos de esquemas son:

- Esquemas basados en firma ciega
- Esquemas basados en mix-nets
- Esquemas basados en cifrado homomórfico
- Esquemas de papeletas precifradas

En el resto de este capítulo se describirán y analizarán estos grupos de esquemas.

4.2 Esquemas basados en firma ciega

En el capítulo 3 se ha explicado la complejidad de cumplir simultáneamente con la autenticación y la privacidad de un votante en un esquema de voto remoto. La autoridad de la elección debe verificar que un votante es legítimo para poder aceptar un voto. Sin embargo, este reconocimiento de la identidad pone en riesgo la privacidad del votante al poder relacionar su identidad con el voto emitido. Para solucionar este problema ha

habido propuestas de separar la autoridad electoral al menos en dos dominios como en el esquema descrito en [Iv91]. En dicho esquema uno de los dominios está a cargo de verificar la identidad del votante y otro dominio recibe y almacena los votos. Esto resuelve el problema de la privacidad en el supuesto de que ambos dominios de autoridad no se confabulen, lo cuál no es ninguna garantía.

A fin de solucionar el problema de privacidad que podría presentarse mediante una confabulación entre los dominios de autoridad, Fujioka y otros [FOO92] propusieron un esquema en donde se utiliza el concepto de firma ciega basado en el trabajo de Chaum [Ch82] para proteger la privacidad del votante. En este y otros esquemas propuestos posteriormente [HMP95, Ok96, Ok97, CC97, OMA+99, XS06] la firma ciega es usada por el votante para que una autoridad de autenticación firme digitalmente el voto cifrado. De esta forma se autoriza la emisión del voto una vez que se ha comprobado la identidad del votante y se protege al mismo tiempo la privacidad de dicho votante. Un esquema basado en firma ciega funciona como se describe a continuación:

Sean los participantes un votante, una autoridad de autenticación y un servidor de votación:

1. El votante escoge su voto V_i y lo cifra con la clave pública (P-E) de la elección:
$$V_i' = (V_i)_{P\text{-}E}$$

2. El votante genera un factor aleatorio de cegado r_i y ciega su voto cifrado:
$$C_i = (V_i')(r_i)$$

3. El votante agrega una prueba de identidad Id_i (credenciales de votante) a su voto cegado y envía el mensaje M_i al servidor de autenticación:
$$M_i = (C_i, Id_i)$$

4. El servidor de autenticación valida los datos de identificación Id_i contenidos en el mensaje y firma digitalmente (con su clave privada *S-A*) el mensaje si el votante es legítimo y no ha votado anteriormente:

$$M_i' = (M_i)_{S\text{-}A}$$

5. El servidor de autenticación envía M_i' al votante como prueba de validación.

6. El votante verifica la firma del servidor de autenticación e invierte el cegado del mensaje:

$$(V_i')_{S\text{-}A} = (M_i')\ (r_i^{-1})$$

7. El votante envía al servidor de votación el voto firmado por el servidor de autenticación:

$$(V_i')_{S\text{-}A}$$

8. El servidor de autenticación verifica la firma del servidor de autenticación y si esta es válida acepta y almacena el voto. Al final de la elección se utiliza la clave privada de la elección para descifrar los votos y llevar a cabo el escrutinio.

La figura 4.1 muestra el intercambio de mensajes entre los tres participantes de un esquema de firma ciega.

Para evitar que la autoridad de autenticación firme digitalmente mensajes no válidos o maliciosos, es decir, que no contengan un voto válido o que el formato no sea el correcto, se utilizan técnicas de "corte y elección" como complemento a la firma ciega, tal como se propone en [RRB00 y UEG01]. Usando estas técnicas, el votante debe generar y enviar a la autoridad de autenticación un conjunto *p* de mensajes cifrados y cegados. La autoridad de autenticación escoge *p-1* mensajes y solicita al votante que le revele los factores de cegado de ese subconjunto de mensajes para comprobar su integridad. Una vez que ha comprobado la integridad de dichos mensajes, la autoridad de autenticación firma el mensaje restante (que aún permanece cegado) y lo envía al votante. El principal problema

es que *p* debe ser lo suficientemente grande para tener una alta probabilidad de detección de mensajes no válidos, por lo que resulta muy costoso computacionalmente el cifrado y cegado de ese conjunto de mensajes.

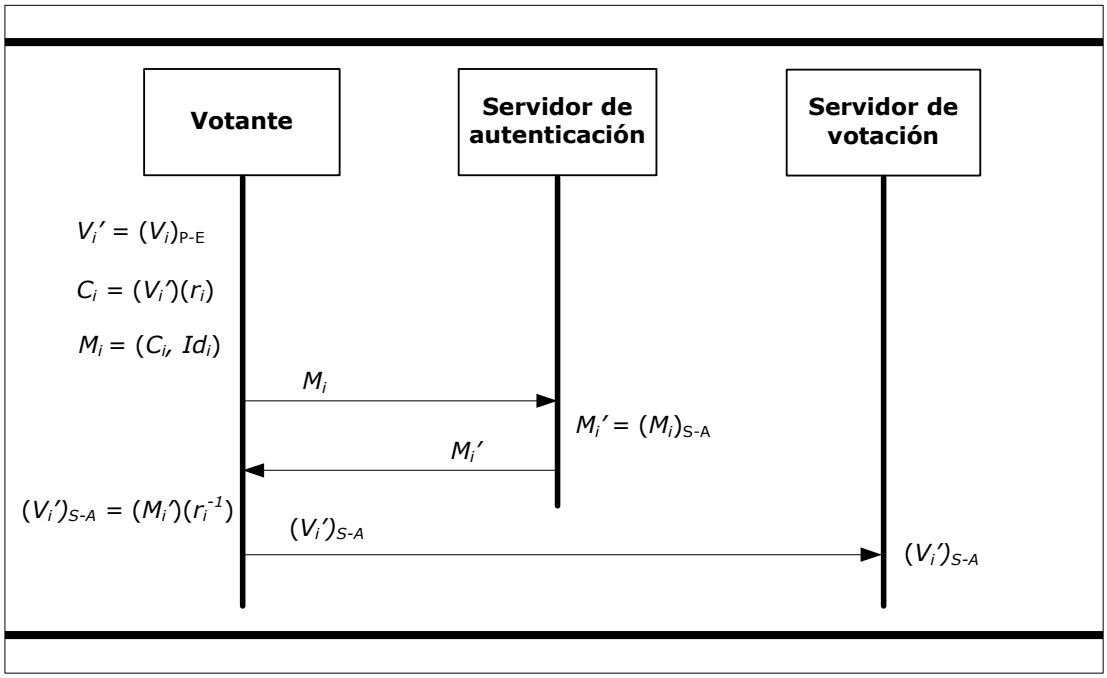

Figura 4.1. Intercambio de mensajes en un esquema de votación genérico basado en firma ciega

Otra desventaja de los esquemas basados en firma ciega es la posibilidad de añadir votos a la base de datos en donde se almacenan. Todos los votos están firmados digitalmente por el servidor de autenticación, por lo que alguien que tenga acceso a la clave privada de dicho servidor puede firmar y añadir votos no legítimos. Finalmente, aún cuando la relación de voto y votante puede protegerse mediante el uso de la firma ciega, dicha relación puede ser descubierta por un atacante que esté monitoreando ambos canales de comunicación, el que se utiliza entre el votante y el servidor de autenticación y el destinado para la comunicación entre el votante y el servidor de votación. Controlando estos canales de comunicación, existe la posibilidad de deducir la relación voto-votante.

4.3 Esquemas basados en mix-nets

Aplicando el concepto de mix-net (que ha sido descrito en el capítulo 2) al voto electrónico, los mensajes son los votos y los emisores de los mensajes son los votantes autorizados. El propósito de la mix-net es romper la relación de los votos cifrados con su origen para evitar que se pueda deducir la relación de un voto con el votante que lo ha emitido. Algunos ejemplos de esquemas de votación con mix-nets los podemos encontrar en [Ab98, Gr03, JJR02, Fu04, MH96, AI03, BG02, Ch04, LBD+03, Ne01, RB99, Ne04, OA00, OKS+97, PBD+04]

4.3.1 Mix-net de descifrado

En el caso de una mix-net de descifrado, se genera una pareja de claves para cada servidor mix participante. El proceso de votación y descifrado se explica a continuación:

1. El votante escoge su voto V_i y lo cifra con las claves públicas de cada servidor mix en el orden inverso de la trayectoria que recorrerá el voto, formando un cifrado anidado. Una vez cifrado, el votante envía su voto al servidor de votación. Supongamos que tenemos n servidores mix, el cifrado sería:

$$V_i^n = ...(((((V_i)_{Pn})_{Pn-1})\ldots_{P2})_{P1})$$

2. Para llevar a cabo el descifrado, el primer servidor mix recibe los votos cifrados y utiliza su clave privada:

$$V_i^{n-1} = ...((((V_i)_{Pn})_{Pn-1})\ldots_{P2})$$

3. El primer servidor mix entonces aplica una función de permutación F sobre la ecuación resultante de su descifrado.

$$F(V_i^{n-1})$$

4. Los votos descifrados y permutados son enviados al siguiente servidor mix, que llevará a cabo las mismas operaciones usando su propia clave de descifrado y su propia función de permutación. Este par de operaciones es repetida por cada servidor hasta que los votos son descifrados.

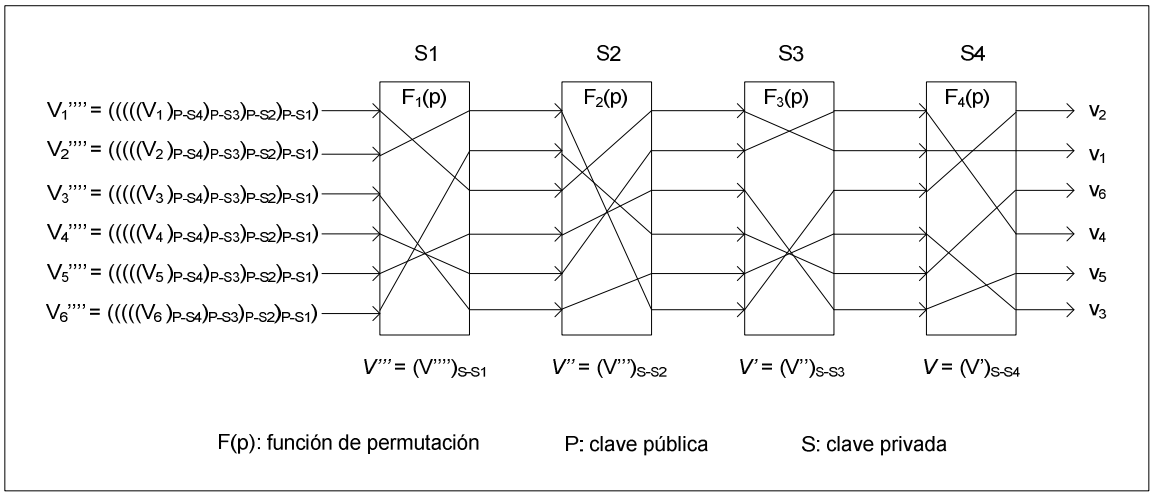

Figura 4.2. Ejemplo de una mix-net de descifrado

La figura 4.2 es un ejemplo de una mix-net de descifrado compuesta de 4 servidores mix y que tiene como entrada 6 votos.

4.3.2 Mix-net de re-cifrado

Por su parte, en las mix-nets de re-cifrado el votante cifra su voto con la clave pública de la mix-net y cada servidor mix vuelve a cifrar el mensaje de manera consecutiva con la misma clave pública. Se muestra a continuación el proceso que se lleva a cabo a partir de la generación del voto por parte de un votante:

1. El votante escoge su voto V_i y lo cifra con la clave pública (P-E) de la elección. Una vez cifrado, el votante envía su voto al servidor de votación. El cifrado sería:

$$V_i' = (V_i)_{P\text{-}E}$$

2. Para llevar a cabo el re-cifrado a través de la mix-net, el primer servidor mix toma el voto cifrado V_i' y lo vuelve a cifrar con la clave pública de la elección:

$$V_i'' = (V_i')_{P\text{-}E}$$

3. Una vez cifrado, el servidor mix aplica una función de permutación F sobre el mensaje resultante:

$$F(V_i'')$$

4. Los mensajes resultantes después de haberlos cifrado y permutado son enviados al siguiente servidor mix. Estas operaciones de re-cifrado y permutación son llevadas a cabo por cada uno de los servidores que integran la mix-net.

5. Al final se tendrá un mensaje que podrá ser descifrado con la clave privada de la elección para recuperar el voto.

En la figura 4.3 se muestra un ejemplo de la forma en que se operarían los votos en una mix-net de re-cifrado.

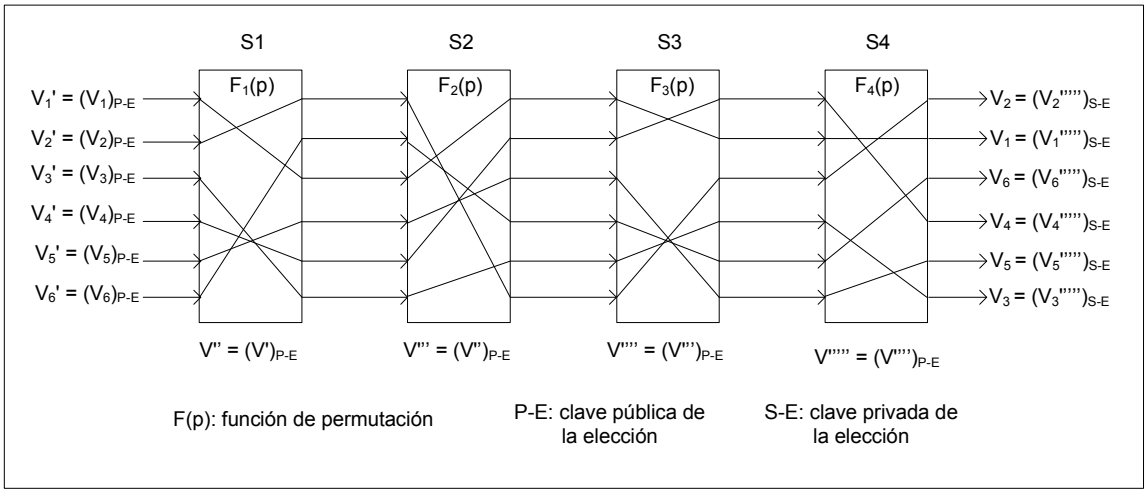

Figura 4.3. Ejemplo de una mix-net de re-cifrado

Para llevar a cabo esta técnica de mix-net se debe utilizar un criptosistema que reúna las características de re-cifrado, es decir, que aún cuando un mensaje se cifre n cantidad de

veces con la misma clave pública, solamente se requiera de un paso de descifrado utilizando la correspondiente clave privada para recuperar el mensaje. Criptosistemas como ElGamal [El84] y Paillier [Pa99] cumplen con esta característica por lo que podrían ser utilizados en este tipo de mix-net.

Bajo cualquiera de las dos implementaciones de mix-net (cifrado o re-cifrado) se logra la privacidad del votante pero siempre con el supuesto de que los servidores mix actuarán honestamente. Las mix-nets de descifrado implican que el votante tenga que llevar a cabo un número de operaciones de cifrado directamente proporcional al número de servidores en la mix-net, lo cuál podría resultar en un alta coste computacional del lado del votante. Por su parte, en una mix-net de re-cifrado, el votante sólo debe llevar a cabo una operación de cifrado, independientemente del número de servidores mix que participan en la elección.

Un problema con ambos tipos de mix-nets es que si se presenta una confabulación de servidores deshonestos, existe el riesgo de violación de la privacidad o de corrupción en la integridad de los votos que recibe el servidor final. Esto surte efecto mediante la sustitución de votos válidos por falsos en alguno de los servidores mix. Existen técnicas de verificación de la operación correcta de los servidores que tratan de prevenir y/o detectar que estas prácticas se lleven a cabo. La verificación en las mix-nets consiste en comprobar que los mensajes recibidos por cada servidor corresponden a los mismos mensajes de salida, con su correspondiente permutación. Una técnica para lograr esto es el uso de pruebas de conocimiento nulo, en dónde cada servidor debe añadir una prueba de compromiso a la permutación de cada voto. Sin embargo, la implementación de pruebas de conocimiento nulo es computacionalmente muy costosa. Jacobsson y otros [JJR02] proponen una técnica de verificación probabilística en la que se verifican aleatoriamente y de manera parcial las entradas y salidas de cierto número de servidores. Esta técnica, aunque efectiva, aún concede un riesgo de que se hayan cambiado algunos mensajes no verificados y que no se detecten dichas manipulaciones.

4.4 Esquemas basados en cifrado homomórfico

Debido a que en muchos esquemas de votación el escrutinio de los votos puede ser considerado simplemente como una suma, el cifrado homomórfico con propiedades aditivas permite hacer dicha suma de los votos. El escrutinio de los votos puede realizarse aún antes de ser descifrados, por lo tanto dicho escrutinio puede llevarlo a cabo alguien que no posee la clave de descifrado, evitando así posibles alteraciones o ataques, y al final descifrar la suma para conocer el resultado.

Por lo general, en este tipo de esquemas el votante envía su voto cifrado a través de un canal público, como un tablón de anuncios electrónico. El voto puede ser descifrado por al menos $t + 1$ autoridades, por lo tanto ningún subconjunto de t autoridades puede conocer el voto. Esto se puede lograr de dos formas:

- Por medio de un criptosistema umbral de clave pública para cifrar los votos. La clave para descifrar los votos es compartida por cualquier conjunto de $t + 1$ autoridades, como en el criptosistema ElGamal.
- El votante comparte su secreto (es decir, su voto) entre N autoridades tal como se describe en [Sc99 y FPS00]. Esto se puede hacer usando un esquema se secreto compartido, como el esquema de Shamir [Sh79]. El votante envía a cada autoridad su secreto cifrado. De esta manera se reduce la posibilidad de ataques provenientes de coaliciones de autoridades deshonestas.

Las propiedades del cifrado homomórfico son utilizadas en diversas propuestas de voto electrónico como [SK94, CFS+96, CGS97, ADG+00, BFP+01, BT94, Be96, DJ01, HS00, KMO01, KY02, LK00, LK02, Ne00, SK94, Sc00].

Cada opción de votación (o candidato) que se presenta al votante debe ser cifrada por éste, con un valor distintivo para saber si el voto debe ser acumulable para un candidato u otro. Por ejemplo, si tenemos dos candidatos posibles A y B, y el votante escoge el candidato A, se realizaría el cifrado para el candidato A con un valor de "1" y el cifrado

para el candidato *B* con un valor de "0". De esta manera, las propiedades aditivas del cifrado homomórfico permitirán llevar a cabo el escrutinio de los votos sin la necesidad de descifrar los votos.

Los esquemas basados en cifrado homomórfico no permiten la gestión de votos abiertos (write-in's), en dónde el votante pueda escoger un candidato diferente a los que se presentan en la lista de candidatos. Tampoco se pueden implementar en elecciones de tipo preferencial, en donde el votante debe escoger sus opciones con un orden de prioridad. Esto se debe a que esos esquemas sólo aceptan valores previamente definidos que permitan llevar a cabo la suma de los votos correctamente, por ejemplo un "1" para el candidato elegido y un "0" para el candidato no elegido. Por esta razón el esquema es funcional básicamente para elecciones con dos candidatos, aunque algunas variantes permiten elecciones con más de dos candidatos.

Adicionalmente, los esquemas de cifrado homomórfico presentan un problema en el que un votante malicioso puede cifrar su voto de tal forma que represente más de un voto para el candidato elegido. Por ejemplo, si en lugar de utilizar un "1" en el cifrado (lo cuál representa un voto), se utiliza un valor "50", se considerarían en el escrutinio cincuenta votos a favor del candidato en lugar de uno solo. Para resolver este problema, se propone que el votante añada una prueba de conocimiento nulo a su voto para comprobar que sus valores usados en el cifrado son "1" para el candidato escogido y "0" para el otro candidato y no un valor diferente que pueda alterar el resultado de la elección. El uso de pruebas de conocimiento nulo hace que el proceso llevado a cabo sea más complejo y muy costoso computacionalmente.

4.5 Esquemas de papeletas precifradas

En un esquema de voto electrónico remoto generalmente se requiere que el votante confíe en un software, el cuál le permite escoger y cifrar el voto antes de enviarlo al servidor de

votación. El ataque más simple contra este tipo de esquemas es la modificación de dicho software para obtener información del voto escogido, con el fin de manipular el voto o simplemente para eliminarlo antes de ser transmitido. El software es proveído por la autoridad electoral o por una tercera parte, pero en cualquier caso el votante debe confiar en que dicho software actuará correctamente.

En el 2000, la "California Internet Voting Task Force" publicó un informe [Ca00] en el que se anticipan los riesgos de seguridad que se podrían presentar en un sistema de voto remoto por Internet. Posteriormente, en un estudio llevado a cabo por Oppliger [Op02] también se hace referencia a esos riesgos y se destacan los posibles ataques contra los ordenadores personales de los votantes. Uno de estos ataques es la inserción de software malicioso en el ordenador del votante, que puede tener como consecuencia la manipulación del voto escogido por el votante. Tanto en [Ca00] como en [Op02] se propone como solución al ataque de inserción de software malicioso el uso de hojas de código (code sheets). El votante debe recibir por medio de correo postal y previo a la fase de votación, una hoja que contiene códigos relacionados a las opciones de voto o candidatos. Durante la fase de votación, el votante debe ingresar el código que corresponde a la opción elegida en lugar de seleccionar directamente la opción o el candidato. Debido a que el software malicioso no tendría acceso a la hoja de códigos, es remotamente probable que pudiera cambiarse el código elegido por el votante por otro código válido, es decir, uno que corresponda a otro de los candidatos. Oppliger [Op02] explica que una apropiada implementación de un esquema de hojas de códigos es una de las principales técnicas para contrarrestar los ataques de software malicioso. Sin embargo, destaca también que existen desventajas como es el hecho de tener que distribuir hojas de código personalizadas, así como el cambio de paradigma que representa para los votantes el tener que votar introduciendo códigos en lugar de seleccionar directamente a un candidato.

Estos esquemas, conocidos posteriormente como "papeletas precifradas" son en principio una buena idea para lograr verificación individual, sin embargo, requieren de otras

características que permitan satisfacer requisitos adicionales de seguridad para el voto electrónico remoto. Esto se evidenciará en esta sección al analizar las propuestas que han surgido a partir del informe en [Ca00].

Las características principales de los esquemas de papeletas precifradas son las siguientes:

- El votante no necesita confiar en un software que lleve a cabo operaciones criptográficas para cifrar y enviar su voto. Este tipo de esquemas no basan su uso en medios convencionales de criptografía del lado del votante. La criptografía utilizada se realiza en una fase previa a la de votación y es llevada a cabo por la autoridad de la elección con el fin de generar las papeletas precifradas.
- El votante no necesita confiar en el ordenador desde el cuál emite su voto. Este es uno de los problemas característicos en un esquema de voto electrónico por Internet. Existen ataques tales como inserción de virus, o software dañino que podría alterar intencionalmente el voto escogido por el votante antes de que éste sea enviado.
- El voto es representado por un código alfanumérico. En algunos casos, el código de votación es acompañado de un código de verificación. Los códigos de votación y verificación son el resultado de operaciones criptográficas.
- Los códigos de votación y verificación son impresos en la papeleta precifrada, la cuál debe entregarse al votante antes de la fase de votación. La autoridad de la elección envía al votante la papeleta precifrada a través de un medio de comunicación independiente presumiblemente seguro (por ejemplo, correo postal).
- Debido a que los códigos de votación y verificación no revelan la opción o candidato elegido por el votante, un ataque de intermediario (man-in-the-middle) no podría llevarse a cabo con éxito. La opción o candidato escogido por el votante se conocerá solamente cuando el código sea descifrado por la autoridad electoral correspondiente al finalizar la fase de votación. Por lo tanto, este tipo de esquemas no requieren de canales anónimos para la transmisión del voto.

- En el caso de los esquemas que utilizan códigos de verificación, el votante puede verificar que su voto ha sido correctamente recibido por el servidor de votación.
- El proceso de votación se puede llevar a cabo desde dispositivos simples con menor poder computacional que el requerido por los esquemas que requieren operaciones criptográficas por parte del votante. Tales dispositivos pueden ser, además de los que pueden disponer de una conexión a Internet: teléfono móvil (mediante SMS), máquinas ATM, teléfono de tonos, entre otros.

La figura 4.4 muestra el protocolo básico de votación llevado a cabo con un sistema basado en papeletas precifradas.

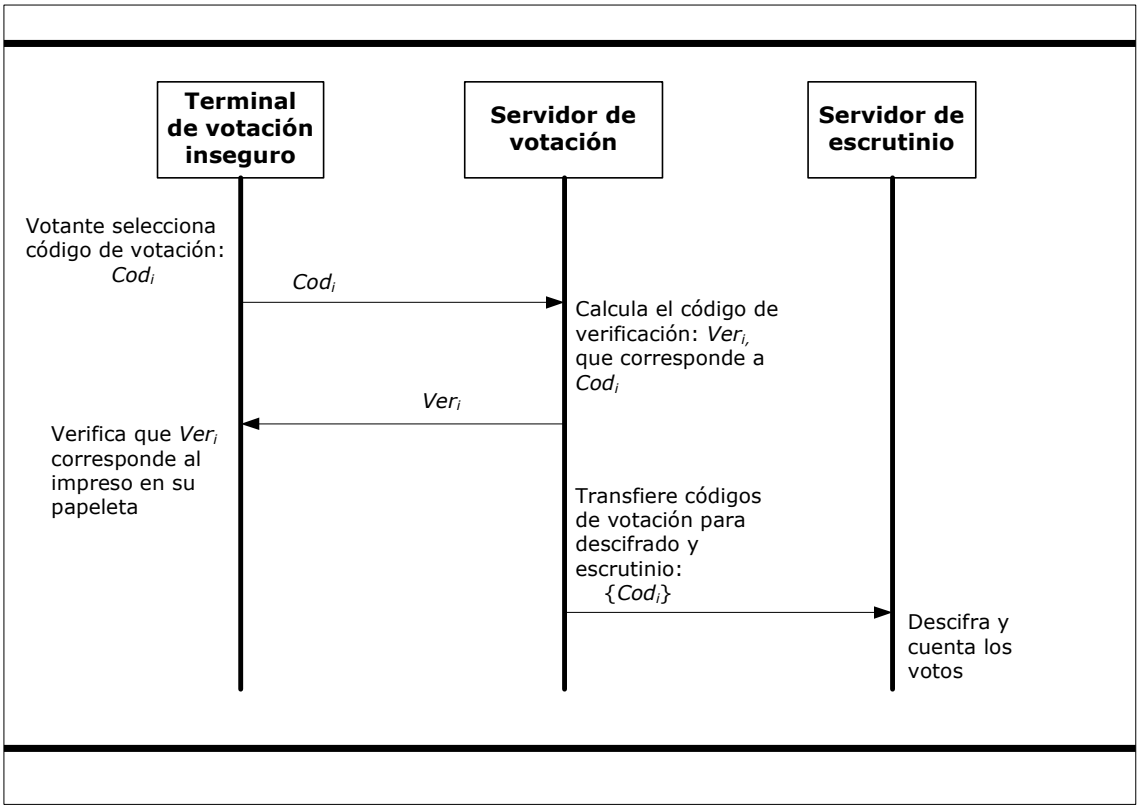

Figura 4.4. Protocolo básico de votación en un esquema de papeletas precifradas

Los esquemas de papeletas precifradas serán analizados con mayor detalle que los esquemas descritos previamente debido a que son de especial interés para la presente investigación. El interés principal en estos esquemas radica en los medios de verificación

que pueden proporcionar al votante, así como la capacidad de prevenir problemas de compromiso del voto en el ordenador del votante. En el capítulo 6 se presentará una propuesta de verificación basada en papeletas precifradas.

A continuación se describen las propuestas de esquemas de papeletas precifradas más importantes a la fecha.

4.5.1 Chaum: Sure-Vote

Chaum propone un sistema de voto electrónico que usa códigos de votación [Ch01], tal como el propuesto en [Ca00]. En este esquema se contempla un código de seguridad (equivalente al código de verificación) asociado a cada código de votación. La papeleta precifrada, que es enviada al votante por un canal seguro, contiene la relación de candidatos con los códigos de votación y con los códigos de seguridad. La papeleta precifrada también contiene un identificador de papeleta. Durante la sesión de voto, el votante envía al servidor de votación el código de votación elegido, entonces se le envía al votante el código de seguridad para que el votante compruebe que éste concuerda con el correspondiente código de seguridad impreso en su papeleta. De esta forma, el votante puede asegurarse que su voto ha sido recibido correctamente por el servidor de votación.

El esquema de Chaum ha sido propuesto inicialmente para voto electrónico presencial a fin de eliminar la necesidad de confianza en los terminales DRE. Sin embargo, en la propuesta se contemplan algunas variantes, como es su uso en un entorno remoto a través de teléfono o de Internet. Además, el sistema contempla como variante la posibilidad de votos abiertos, ya que se puede usar un código especial para una opción de voto no contemplada en la papeleta. Sin embargo, el esquema no contempla medidas de seguridad en la generación de los códigos de votación y de seguridad que ayuden a preservar la privacidad de los votos. Por otro lado, aún cuando el votante puede verificar que su voto se ha registrado correctamente, no existe una forma en que pueda verificar que el voto ha sido incluido en el escrutinio.

4.5.2 Malkhi: voto electrónico "sin criptografía"

Malkhi y otros [MMP02] propusieron un esquema que está basado en un concepto de vectores de verificación. Los participantes del esquema son: un conjunto de autoridades de registro, los votantes y un conjunto de autoridades de escrutinio. Una autoridad de registro entrega al votante un conjunto de vectores (las opciones de voto o candidatos) junto con un secreto S para ese grupo de vectores. El voto enviado por el votante a la autoridad de escrutinio es un vector V. Entonces, la autoridad devuelve al votante un vector de verificación B. El votante entonces verifica que $(V)(B) = S$. De esta manera, el votante puede verificar que su voto se ha recibido correctamente. El esquema requiere de canales seguros de comunicación entre el votante y las autoridades electorales.

A continuación se describe el proceso llevado a cabo en cada una de las fases que conforman el esquema:

- Registro. Los vectores de verificación son usados por las autoridades de registro para repartir a los votantes sus conjuntos de vectores secretos V, el secreto S, y el identificador de votante *vid*. También son usados para enviar los correspondientes vectores a la autoridad de escrutinio. A cada votante se le asignan varios pares de vectores $\{(V_{1,0}; V_{1,1}), (V_{2,0}; V_{2,1}),\ldots\}$ a fin de tener la posibilidad de hacer pruebas de que los votos son recibidos por la entidad correcta antes de enviar el voto definitivo, tal como se explica en el siguiente paso.

- Prueba. En esta etapa los votantes tienen la posibilidad de asegurarse que la autoridad que recibe los votos posee los vectores de verificación B correctos. El votante selecciona aleatoriamente uno de los vectores V, por ejemplo $V_{1,0}$ y lo envía a diferentes autoridades de escrutinio. Cada autoridad de escrutinio debe devolver al votante el vector de verificación correspondiente al vector adyacente al enviado, en este caso el vector de verificación sería $B_{1,1}$. El votante entonces

verifica que $(B_{1,1})(V_{1,1}) = S$. Los pares de vectores usados para prueba deben ser publicados a fin de que ya no puedan ser usados para la votación.

- Votación. El votante envía el vector que corresponde al candidato elegido, junto con su identificador de votante *vid* a diferentes autoridades de escrutinio. Cada autoridad verifica que el producto del vector recibido y el vector de verificación corresponde a *S*. Hecho esto, el vector de verificación enviado al votante será el que corresponde al vector adyacente. De esta manera el votante puede verificar que $(V)(B) = S$.

- Escrutinio. Al final de la elección, cada autoridad de escrutinio publica los vectores recibidos y los *vid*. Por lo tanto, cada una de las autoridades de escrutinio puede verificar la validez de los vectores recibidos por las demás autoridades e incluso realizar el escrutinio de los votos que han sido recibidos por todas las autoridades. De esta manera se puede llevar a cabo el escrutinio de la elección.

En este esquema, el votante aún necesita ejecutar una cantidad de cómputo considerable para verificar que su voto se ha recibido correctamente. Por otro lado, la verificación conseguida por el votante se limita a que este puede asegurarse que el voto fue recibido por la entidad correcta y sin haber sido alterado antes o durante la transmisión. Sin embargo, el esquema no contempla que las autoridades de escrutinio puedan actuar deshonestamente o incluso que pueda haber ataques que modifiquen el voto una vez que este ha sido recibido por dicha autoridad. Aún así, esta propuesta ha servido como punto de partida para otras propuestas de sistemas de papeletas precifradas.

4.5.3 Propuesta del CESG

El CESG (grupo de seguridad de comunicaciones y electrónica del Reino Unido) ha propuesto un esquema de papeletas precifradas [CESG02] específicamente para

elecciones generales del Reino Unido. Se asume que existe un registro previo de votantes. Los pasos del esquema se describen a continuación:

- Pre - elección. La autoridad electoral lleva a cabo tareas de preparación para la elección. Entre estas tareas se encuentra la generación, mediante operaciones criptográficas, de las identificaciones de los candidatos así como los valores que serán impresos en la papeleta. El votante recibe una papeleta precifrada como la de la figura 4.5. Se asume que la papeleta precifrada se ha impreso de una forma segura y se sugiere que sea enviada al votante a través de correo postal. La papeleta contiene el nombre del votante, un número de identificación del votante (*vid*) así como información de los candidatos nominados, además de un número de identificación de candidato *PCIN* (equivalente al código de votación de otros esquemas) y un número de identificación de retorno *RID* (equivalente al código de verificación) asociados a cada candidato. Estos valores son generados por la autoridad electoral mediante funciones unidireccionales.

- Votación. En la fase de voto, el votante envía al servidor de votación su voto compuesto por su *vid* y el *PCIN* del candidato elegido. El servidor de votación calcula el *RID* que corresponde y lo envía al votante por el mismo canal de comunicación que recibió el voto. El votante entonces confirma que el *RID* recibido coincide con el *RID* impreso en la su papeleta precifrada y que corresponde al candidato elegido. Por ejemplo, si el votante envía el mensaje "3984793 36975", indica que el candidato seleccionado es "Carlos Calderón".

- Escrutinio. La autoridad de escrutinio lleva a cabo las operaciones necesarias para determinar a qué candidato corresponde cada *PCIN* recibido durante la elección. De esta manera se puede determinar el resultado de la elección.

En este esquema, al igual que los descritos anteriormente, aún cuando el votante verifica que su voto se ha recibido correctamente, no hay garantía de que el voto será incluido apropiadamente en el escrutinio, por lo tanto el esquema no cumple completamente con

el requisito de verificación individual. Por otro lado, la autoridad de la elección no puede probar que un votante no ha emitido su voto. Por lo tanto, un votante malicioso puede asegurar haber votado (sin haberlo hecho) y que ha recibido el código de verificación correcto y la autoridad de la elección no puede comprobar lo contrario. Además, dado que la autoridad de la elección conoce la relación de identificadores de votante con los identificadores de candidatos, la privacidad del voto esta expuesta a ser violada, o bien, estos datos pueden ser utilizados para agregar votos en nombre de los votantes que no votaron.

Nombre del votante: Carlos Pérez

Identificador de votante: 3984793

Candidato	Código de votación	Código de verificación
Carlos Calderón	36975	8473313
Andres Salinas	64847	2748473
Felipe López	82935	4865393

Figura 4.5. Ejemplo de papeleta precifrada

4.5.4 Storer: mCESG

En [SD04a y SD04b], Storer trata de mitigar los defectos identificados en [CESG02], los cuáles ya han sido destacados previamente en la sección 4.5.3. Para contrarrestar los problemas de verificación por parte del votante, Storer propone el empleo de un tablón electrónico. En dicho tablón se publican los *RID* de los votos que se van recibiendo durante la fase de votación. En el mismo tablón electrónico se publican, al cierre de la votación, los nombres de los candidatos que corresponden a los *RID*, de tal manera que el votante pueda verificar que su voto ha sido asociado al candidato correcto.

Por otra parte, a fin de mitigar el problema de la privacidad del voto se propone la distribución de las funciones de la autoridad electoral en diferentes dominios autónomos. La papeleta precifrada es generada por más de una autoridad, haciéndola mas segura frente a posibles ataques de la propia autoridad de la elección. Dichos ataques son los referentes a violación de la privacidad y posibilidad de que la autoridad utilice los datos de las papeletas pertenecientes a votantes que no votaron para emitir votos extras al cierre de la elección. Los dominios de autoridad son establecidos como se describe a continuación:

- Oficial de registro, el cuál se encarga de administrar la identidad de los votantes. Recaba la información de los votantes y genera los identificadores de votante *vid*. También se encarga de distribuir a los votantes una parte de la papeleta precifrada.
- Oficial de retorno, el cuál es responsable de administrar la identidad de los candidatos. Este recibe la información de candidatos y genera los identificadores para cada uno de los candidatos.
- Oficial de votación, encargado de generar la mayor parte de los elementos de la papeleta precifrada y de recibir los votos durante la elección.
- Comisión electoral, la cuál es responsable de entregar a cada votante una tarjeta de seguridad conteniendo el resto de elementos necesarios para la votación.
- Distribuidor de PCIN's (número de identificación de candidatos).

El protocolo propuesto en [SD04a y SD04b] funciona de la siguiente manera:

1. Al igual que en el esquema CESG original [CESG02], cada votante recibe una papeleta precifrada tal como la que se muestra en la figura 4.5. Sin embargo, en este esquema, el votante recibe su papeleta en tres documentos separados. El primero es entregado por el oficial de registro y contiene los datos del votante (nombre e identificador) y los nombres de los candidatos. El distribuidor de PCIN's, por su parte debe entregar los valores *PCIN* y la mitad de dígitos de los valores *RID*. Finalmente, la comisión electoral se encarga de entregar la mitad restante de los valores *RID*. Al recibir los tres documentos, el votante los junta para formar su papeleta precifrada.

2. El protocolo de votación, al igual que en [CESG02], requiere que el votante envíe al servidor de votación su *vid* y el *PCIN* correspondiente al candidato de preferencia.

3. En lugar de devolver al votante el valor *RID* que corresponde a su voto enviado, dicho valor se adhiere a un listado público al que se puede acceder a través de un sitio Web. Por lo tanto, los votantes y cualquier observador puede ver los *RID* que se van publicando durante la votación. Si después de un tiempo razonable el votante no ve publicado el *RID* que corresponde a su voto enviado, debe contactar a la autoridad electoral para determinar si ha ocurrido alguna falla, por ejemplo que el voto no ha sido recibido.

4. Al cierre de la elección, son publicados en el mismo sitio Web los nombres de los candidatos que corresponden a cada uno de los *RID* publicados durante el periodo de votación. Entonces el votante debe verificar que la relación *RID*–candidato corresponde a la impresa en su papeleta precifrada. Si hubiera alguna discrepancia en la correspondencia, el votante puede quejarse al respecto.

El diseño de separación de dominios de autoridad descrito en este esquema no asegura en sí mismo la protección de la privacidad del votante ya que bastaría una confabulación entre autoridades para lograr algún ataque exitoso. Por otro lado, el hecho de que exista un tablón electrónico público en el que votante pueda verificar su *RID* relacionado al candidato elegido presenta una gran oportunidad de coerción a gran escala, ya que el atacante puede verificar que el votante ha votado como se le ha indicado simplemente teniendo una copia de la papeleta precifrada y accediendo al tablón electrónico al final de la elección.

4.5.5 Storer: variantes del esquema mCESG

Posteriormente, Storer [SD05] propuso un par de variantes para el esquema descrito en [SD04a y SD04b]. La primera variante se enfoca en adaptar el esquema original a elecciones preferenciales, es decir, en elecciones en las que el votante debe seleccionar cierta cantidad de candidatos en orden de preferencia en lugar de seleccionar sólo uno. La finalidad de esta variante es utilizar el mismo tipo de papeleta precifrada con la adición de una cantidad mínima de nuevos elementos.

Con la segunda variante se trata además de prevenir ataques de coerción. Esto se hace también agregando nuevos elementos en la papeleta precifrada. A continuación se explica detalladamente cada una de estas variantes.

Para emplear el esquema en elecciones preferenciales, la papeleta precifrada debe contener de manera adicional:

- *n* dígitos asociados al orden de preferencia de *n* candidatos que se presentan como parte del código *PCIN*. Cada *PCIN* tiene, por lo tanto n dígitos adicionales, los cuáles son diferentes para cada candidato impreso en la papeleta.
- *n* dígitos asociados al orden de preferencia de n candidatos que se presentan como parte del código *RID*. De igual forma que los *PCIN,* los *RID* tienen *n* dígitos adicionales, los cuáles son diferentes para cada candidato impreso en la papeleta.
- Un conjunto de números de comprobación (checksums) que varían según el número de candidatos escogidos. Por ejemplo, si el votante escoge a dos candidatos, entonces el número de comprobación correspondiente es el asociado con el número 2.

Un ejemplo de dicha papeleta precifrada se muestra en la figura 4.6. Los dígitos entre los símbolos { } permiten indicar la preferencia sobre un candidato en una elección de tipo

preferencial. En base a este ejemplo podemos construir el mensaje enviado por un votante de la siguiente manera:

"3984793 64847 86935 948"

en donde:

- "3984793" es el identificador del votante

- "64847" indica que el votante ha seleccionado al candidato "Andrés Salinas". El segundo dígito indica que este candidato es el número 1 en la preferencia del votante.

- "86935" indica que el votante ha seleccionado al candidato "Felipe López" como segunda opción en su preferencia, lo cuál se representa con el número 6 en el segundo dígito.

- "948" denota el número de comprobación e indica que el votante ha seleccionado a dos candidatos.

Nombre del votante: Carlos Pérez

Identificador de votante: 3984793

Números de comprobación:
1: 647
2: 948
3: 245

Candidato	**Código de votación** {1, 2, 3}	**Código de verificación** {1, 2, 3}
Carlos Calderón	3{6, 4, 7}975	847{3, 9, 7}313
Andres Salinas	6{4, 2, 9}847	274{8, 7, 4}473
Felipe López	8{2, 6, 3}935	486{5, 4, 8}393

Figura 4.6. Ejemplo de papeleta precifrada en el esquema de variantes del mCESG

Para que el esquema esté libre de coerción, el autor propone separar la asociación entre votantes y candidatos elegidos. Para lograr esto, a cada votante se asigna un número personal de respuesta (*PRN*, por sus siglas en inglés) que debe ser único. Este número es incluido en la papeleta precifrada. Además, el código de respuesta asignado para cada

candidato es pequeño y no necesariamente único. Este código es el llamado *RID* en los esquemas anteriores, y en este esquema introducido con el término *CRN* (candidate response number).

Aún con las variantes propuestas, la generación y distribución de las partes de la papeleta precifrada está a cargo de los dominios de autoridad ya definidos en el esquema original [SD04a, SD04b]. El procedimiento de envío del voto también se mantiene igual que en el esquema original. Sin embargo, las diferencias están en el proceso de verificación, el cuál en este esquema se lleva a cabo en tres fases:

- La primera fase de verificación se lleva acabo durante la votación. En esta fase se publican en un tablón electrónico los *PRN* de los votantes que han enviado su voto. Por lo tanto, en esta etapa el votante puede saber que se ha recibido su intención de voto, aunque sin tener la certeza de que el voto se ha registrado correctamente.
- La segunda fase de la verificación se lleva a cabo al terminar el periodo de votación. Esta verificación se realiza en un ambiente aislado, en el cuál, un grupo de oficiales de la elección, junto con los candidatos o sus representantes, revelan la asociación de *PRN's, CRN's* e identidades de los candidatos. Una vez revelada dicha asociación, los candidatos seleccionan un pequeño subconjunto de datos para ser publicados en el tablón electrónico. Lo que se publica inicialmente es la relación de *PRN's* y *CRN's* para que los votantes verifiquen que su *PRN* está relacionado al *CRN* correspondiente al candidato elegido y el cuál se encuentra impreso en la papeleta. Debido a que sólo se publican el subconjunto de asociaciones escogidas por los candidatos, sólo el subconjunto correspondiente de votantes podrá encontrar sus valores publicados.
- Si los votantes que pudieron verificar sus valores publicados en la fase anterior no tienen alguna objeción, se lleva a cabo la tercera fase de la verificación. En esta fase la autoridad de la elección publica la relación entre *CRN's* e identidades de los candidatos. Una vez más, el subconjunto de votantes que ha podido verificar la correspondencia de su *PRN* con el *CRN*, pueden verificar en esta fase que la

identidad del candidato publicada corresponde al candidato elegido en el proceso de votación.

Una de las claves de este proceso de verificación es el tamaño del subconjunto escogido para llevar a cabo la verificación completa. Si el número elegido es muy pequeño, entonces la autoridad de la elección tiene una probabilidad alta de llevar a cabo una manipulación en el proceso sin ser descubierta. Por otro lado, entre más grande sea el número de votantes que pueden verificar su voto, será mayor la probabilidad de que se presenten ataques exitosos de coerción.

Otro problema a destacar es el limitado número de votantes que tiene la posibilidad de verificar el correcto tratamiento de su voto, por lo que el esquema al tratar de evitar coerción pierde fiabilidad. Si bien es cierto que probabilísticamente se puede comprobar que aún con un número bajo de votantes que verifican su voto es posible detectar un número elevado de manipulaciones, la percepción para los votantes que no tienen la posibilidad de verificar el correcto tratamiento de su voto puede ser diferente.

4.5.6 Voutsis: códigos de votación para voto desde dispositivos móviles

Voutsis y Zimmermann [VZ05] también proponen un esquema basado en códigos de votación. Al igual que en las propuestas mencionadas anteriormente, la criptografía es utilizada para la generación de los códigos de votación, por lo que el votante no requiere de un dispositivo de alto poder computacional para enviar su voto. De hecho, en la implementación que se describe en la propuesta, el voto es enviado a través de mensaje de texto de telefonía móvil.

El esquema se desarrolla de acuerdo a los siguientes pasos:

1. Inicialización. Durante la fase inicial se generan los códigos de votación y se distribuyen junto con las credenciales de votante. Las credenciales de votante

podrían ser por ejemplo un código de identificación y una contraseña, las cuáles son impresos en la papeleta precifrada. Otra opción de identificación sería a través de tarjetas inteligentes. Los pasos llevados a cabo en la inicialización del sistema se muestran a continuación. En la propuesta se habla de más de una opción para llevar a cabo algunos de los pasos, sin embargo, aquí se describe sólo la opción más genérica:

- Cifrado de las respuestas. Cada posible respuesta es primeramente representada de manera binaria. Para hacer esto, las respuestas se indexan y entonces el índice decimal se convierte a su representación binaria, tal como se muestra en la tabla 4.1. La representación binaria de cada posible respuesta se hace anónima añadiendo bits aleatorios de relleno, por ejemplo al inicio y al final de la cadena de bits de la respuesta. Una vez que se tiene una cadena de bits anónima se cifra con un algoritmo de clave pública. Se sugiere que el cifrado se lleve a cabo con dos claves públicas diferentes (cuyas claves privadas se asignan a dos autoridades de la elección) para no conceder la responsabilidad total a una sola autoridad. Este procedimiento de hacer anónimas las respuestas y después cifrarlas se lleva a cabo un número grande de veces, de preferencia tan grande como el número de votantes potenciales. De esta manera cada votante tendría códigos de votación únicos.

Tabla 4.1. Precifrado de las opciones de votación

Respuestas	Índice	Binario
“si”	1	00000001
“no”	2	00000010
…		
“abc”	7	00000111
“def”	8	00001000

- Generación y asignación de códigos. Cada cadena cifrada se mapea con una cadena única y aleatoria de caracteres. El resultado de este mapeo, junto con un carácter de control, son los códigos de votación tal como serán entregados al votante. Los mapeos realizados se almacenan en una tabla que será usada al cierre de la elección para llevar a cabo el descifrado y escrutinio de votos.

- Impresión de las papeletas precifradas. Se toman de manera aleatoria las listas de códigos previamente generadas y se asignan a las correspondientes respuestas para cada papeleta. Una vez impresas, se elimina cualquier información que pudiera relacionar las respuestas con los códigos. La única evidencia de relación sería la propia papeleta.

2. Votación. El votante envía el código de votación junto con sus credenciales. Cuando el servidor de votación recibe el código, primeramente se verifica el carácter de control para asegurarse que el código recibido es un código válido. Después se verifica la correcta identidad del votante. Una vez que ambas comprobaciones han sido validadas, se separan los datos de identidad del votante del código de votación.

3. Escrutinio. Para llevar a cabo el escrutinio, los códigos de votación recibidos son inversamente mapeados a las correspondientes respuestas cifradas. Entonces las respuestas son descifradas con la o las claves privadas de las autoridades electorales que participaron en el cifrado y por último son eliminados los bits de relleno para obtener las respuestas y llevar a cabo el escrutinio.

El hecho de que los códigos de votación contienen un carácter de control evita que las papeletas precifradas puedan ser manipuladas al cambiar algún código por uno no válido. Sin embargo todavía se puede llevar un ataque de manipulación de la papeleta al cambiar entre sí dos o más códigos de votación, de tal manera que queden asignados a una respuesta diferente a la originalmente asignada. Debido a que en este esquema no se contemplan códigos de verificación para que el votante verifique que el voto se ha

recibido correctamente, este ataque no sería detectado ni por el votante ni por la autoridad de la elección.

4.5.7 Joaquim: protección contra voto automatizado

Joaquim y Ribeiro [JR07] también enfocan su propuesta de papeletas precifradas a la mitigación de los problemas de seguridad ligados al voto electrónico remoto, y más específicamente a los riesgos de seguridad en el ordenador del votante. En este esquema se propone una interfaz basada en papeletas precifradas para que el votante escoja su voto de una manera segura. Por lo tanto, el esquema debe adaptarse a un sistema de votación que lleva a cabo el resto de las operaciones del proceso de votación, como el envío del voto al servidor de votación, escrutinio, etc.

En el esquema existe una fase de generación de las papeletas que incluye códigos de votación (papeleta precifrada). La diferencia con los esquemas descritos anteriormente, es que en este, además de imprimir la relación de candidatos con los códigos de votación, dicha relación también es almacenada en una tarjeta inteligente. Por lo tanto, a cada votante se le entrega la papeleta precifrada impresa y el equivalente en una tarjeta inteligente. Dicha tarjeta también contiene un certificado digital del votante que sirve para llevar a cabo su autenticación frente al sistema. Durante la sesión de voto, el votante ingresa el código de votación correspondiente al candidato elegido tal como aparece en su papeleta impresa. Este código es enviado localmente a la tarjeta inteligente y esta realiza la conversión del código de votación al candidato. A partir de aquí tendría que usarse una aplicación que lleve a cabo un protocolo de votación para el resto de las operaciones. La aplicación deberá comunicar a la tarjeta inteligente cuando el voto ha sido entregado al servidor de votación, para que la tarjeta a su vez lo notifique al votante mediante un código de confirmación de voto, el cuál también está impreso en la papeleta. Por lo tanto el votante podría estar seguro que su voto se ha emitido. Tal como se ha explicado, la tarjeta inteligente juega un papel importante en el esquema, ya que es en este dispositivo en el que se está confiando la correcta emisión del voto.

El esquema cumple con su propósito, que consiste en que el voto sea enviado sin alteraciones por parte de alguna aplicación maliciosa hospedada en el terminal de votación. Sin embargo, la verificación de que el voto sea recibido y contado correctamente va más allá de su alcance y queda expuesta al protocolo de votación utilizado.

4.5.8 Evaluación de los esquemas de papeletas precifradas

Las propuestas de papeletas precifradas descritas en esta sección tratan principalmente de mitigar un problema. Este problema es el riesgo de que software malicioso sea insertado en el terminal de votación (usualmente un ordenador personal) con la finalidad de conocer o alterar el contenido del voto antes de ser enviado al servidor. En términos generales, a través de un código de verificación el votante puede asegurarse que su voto fue registrado correctamente. La segunda parte de la verificación (inclusión del voto en el escrutinio) es omitida en la mayoría de las propuestas. En [SD05] se incluye un método de verificación de inclusión del voto en el escrutinio, sin embargo tal como se ha descrito en el análisis de dicha propuesta en la sección 4.5.5, la verificación es selectiva, es decir, solamente un subconjunto de votantes puede verificar el correcto tratamiento de su voto.

Por otro lado, existen riesgos de seguridad tanto en la generación como en la distribución de las papeletas precifradas. La relación entre códigos de votación y candidatos puede llegar a ser conocida por algún oficial o personal técnico involucrado en la elección si no se cuenta con medidas de seguridad apropiadas durante el proceso de generación de los códigos de votación. Además, las papeletas precifradas podrían ser alteradas sin la detección del votante, de modo que el voto enviado puede ser diferente a la intención real del votante. Los esquemas de papeletas precifradas pueden también enfrentar problemas de usabilidad. En un esquema de voto electrónico, el votante usualmente escoge su opción o candidato a través de un click o incluso tocando la opción, nombre o fotografía del candidato en una pantalla sensible al tacto. Sin embargo, en un esquema de papeleta precifrada los votantes tienen que introducir, a través de un teclado, el código de votación correspondiente al candidato. Esta situación podría ser un inconveniente para algunos

votantes, especialmente en elecciones múltiples, es decir, en elecciones en donde se tiene que votar en la misma sesión por más de un propósito, por ejemplo por un presidente, por un diputado y por un alcalde.

4.6 Comparativa de esquemas de voto electrónico remoto

En este capítulo se han descrito una variedad de esquemas propuestos para el voto electrónico remoto basados en mecanismos criptográficos. En la tabla 4.2 se hace un resumen de las ventajas y desventajas de dichos esquemas en base a la clasificación ya descrita.

Tabla 4.2. Resumen de ventajas y desventajas de los esquemas de voto electrónico remoto

Clasificación	Ventajas	Desventajas	Ejemplos de Propuestas
Esquemas basados en firma ciega	Protegen la privacidad del votante al separar los procesos de autenticación y de voto.	- La protección del anonimato puede verse afectada si un atacante monitorea el canal de comunicación. - Con el conocimiento de la clave privada de la autoridad de autenticación, se pueden añadir votos no legítimos.	[FOO92, XS06, Mo08]
Esquemas de mix-nets	Protegen la privacidad del votante a través de las permutaciones llevadas a cabo.	- Difícil verificación de que los servidores mix han actuado correctamente. - En el caso de mix-net de descifrado el terminal de votación requiere de alta capacidad de cómputo.	[Ab98, JJR02, Ne04]
Esquemas de cifrado homomórfico	Protegen la privacidad del votante al no tener que descifrar los votos individualmente para llevar a cabo el escrutinio.	- No soportan todo tipo de elecciones. - Son susceptibles a ataques en donde votantes deshonestos pueden enviar un mensaje que represente más de un voto para un candidato.	[SK94, HS00, Sc00]

Tabla 4.2 (*continuación*). Resumen de ventajas y desventajas de los esquemas de voto electrónico remoto

Clasificación	Ventajas	Desventajas	Ejemplos de Propuestas
Esquemas de papeletas precifradas	- Protegen la privacidad del votante ya que este envía como voto un código cuya relación con el candidato es desconocida para el servidor de votación. - Evitan ataques de código malicioso que trate de alterar o conocer el contenido del voto. - El voto puede ser enviado desde un dispositivo con baja capacidad de cómputo. - Permiten al votante verificar que su voto se ha recibido correctamente en el servidor de votación.	- Posibles alteraciones en las papeletas precifradas sin detección, lo cuál ocasionaría que el votante envíe un voto diferente al deseado. - Se pueden presentar problemas de logística en la distribución de las papeletas a los votantes. - Votantes no pueden verificar que su voto fue incluido en el escrutinio sin arriesgar un ataque de coerción masiva. - Poca usabilidad al tener que teclear códigos de votación.	[Ch01, CESG02, JR07]

4.7 Conclusiones

Tal como se ha analizado en este capítulo y como se puede ver de manera resumida en la tabla 4.2, los cuatro grupos de esquemas analizados cuentan con importantes características que permiten satisfacer los requisitos de seguridad en el voto electrónico remoto. Cada uno de estos grupos de esquemas tratan dichos requisitos en distintas maneras, sin embargo, la principal aportación de los tres primeros (firma ciega, mix-nets y cifrado homomórfico) es la forma en cómo logran satisfacer el requisito de privacidad. Los esquemas de firma ciega, tal como se ha analizado, logran satisfacer la privacidad de los votantes al separar las entidades de autenticación y recepción del voto. Los esquemas basados en mix-nets abordan el problema de la privacidad llevando a cabo una serie de transformaciones de los votos (cifrados y permutaciones) para eliminar la relación entre votos y votantes. Por su parte, los esquemas basados en cifrado homomórfico utilizan las propiedades homomórficas de algunos criptosistemas que permiten obtener los resultados de la elección sin la necesidad de descifrar los votos individualmente, garantizando de

esta forma la privacidad de los votantes. Sin embargo, los tres esquemas presentan el riesgo de que un voto pueda ser conocido por un atacante, e incluso manipulado, en el terminal de votación antes de que se lleve a cabo el cifrado del voto. Este ataque se puede llevar a cabo insertando software malicioso en el terminal de votación, por ejemplo en el ordenador del votante.

Los esquemas de papeletas precifradas logran la privacidad de los votantes incluso frente a ataques de inserción de software malicioso en el ordenador del votante, ya que los votos son escogidos a través de un código de votación que no revela información de la opción escogida por el votante. Además, los esquemas de papeletas precifradas proporcionan algunas ventajas adicionales enfocadas en la verificación de los votos. Bajo un esquema de papeletas precifradas que utiliza códigos de verificación, el votante puede asegurarse que su voto ha sido recibido correctamente por el servidor de votación. Sin embargo, los esquemas de papeletas precifradas propuestos a la fecha no permiten el votante verificar de una manera eficiente que su voto ha sido incluido correctamente en el escrutinio de los votos. Por otro lado, los esquemas de papeletas precifradas presentan algunos retos, especialmente relacionados con la generación de las papeletas y la distribución de las mismas a los votantes. Otro problema a considerar es el de la usabilidad de un sistema de votación basado en un esquema de este tipo, el cuál podría restringir su uso a determinados tipos de elecciones. En el capítulo 6 se presenta un esquema de verificación individual basado en papeletas precifradas. En dicho esquema los votantes tienen la posibilidad de verificar (además del registro correcto de su voto en el servidor de votación) que su voto ha sido apropiadamente incluido en el escrutinio. De esa manera se resuelve el problema principal de los esquemas actuales de papeletas precifradas.

Capítulo 5

Registro Remoto de Votantes

5.1 Introducción

Debido al creciente interés para mejorar la eficiencia en los sistemas electorales, en los últimos años se han estado considerando distintas vías para automatizar los diferentes procesos implicados en una elección. Estas mejoras han dado como resultado un amplio rango de propuestas de esquemas aplicados a los diferentes procesos de una elección. La mayoría de esas propuestas se han enfocado principalmente en la fase de votación de una elección. Sin embargo, existen otros procesos que pueden llevarse a cabo utilizando medios electrónicos, como el registro de votantes.

El registro de votantes es el proceso de recolección de los datos de los votantes a fin de constituir un censo electoral. También existen fases dentro del proceso de registro en las que se constituyen subconjuntos del censo electoral que determinan el canal de votación escogido por el votante para una elección específica. Debido al hecho de que el censo electoral determina si un votante tiene derecho a votar en una elección o por un canal de votación en particular, debe ser creado de una manera eficiente y segura. Aún cuando otros procesos de una elección cuenten con medidas de seguridad (por ejemplo los procesos de votación o escrutinio de los votos), un registro de votantes deficiente puede facilitar el llevar a cabo prácticas fraudulentas que afectan a la integridad de los resultados de la elección.

El registro de votantes es usualmente llevado a cabo de manera presencial ante un oficial de registro. Dicho proceso presenta algunas variantes entre países, a continuación se presentan algunos ejemplos:

- En algunos países como los Estados Unidos o el Reino Unido se debe formar un censo electoral de manera previa a cada elección, por lo tanto los votantes deben llevar a cabo su registro dentro de cierto periodo previo a la elección.
- En otros países como es el caso de España, el censo electoral se genera automáticamente a partir de los registros de población. Los votantes tienen la posibilidad de verificar de manera anticipada a la elección si su registro aparece de manera correcta en el censo electoral y si fuera necesario pueden solicitar alguna corrección al registro.
- Otra variante es como el caso de México, en dónde los ciudadanos que cumplen la mayoría de edad deben llevar a cabo su registro en el censo electoral y ese registro será usado para cualquier elección. En este caso el ciudadano debe notificar en una oficina de registro cuando se produzca un cambio en su domicilio con el fin de que cuando se presente una elección, el votante tenga asignado el colegio electoral correcto.

En cualquiera de estas variantes en el proceso de registro, el votante interactúa directamente con un oficial de registro. En el primer caso, antes de cada elección. En el segundo caso sólo cuando es necesario llevar a cabo alguna modificación al registro, y en el tercer caso, al menos una vez cuando el ciudadano lleva a cabo su registro inicial.

Esta tarea se vuelve más compleja cuando hay votantes que no pueden acudir ante un oficial de registro, por ejemplo los residentes en el extranjero, por lo que es necesario implementar métodos seguros y eficientes de registro remoto. Además, es indispensable considerar que con la implementación de sistemas de voto remoto también resulta necesaria la adopción de sistemas de registro de votantes que utilicen canales de comunicación remotos.

Los sistemas de registro remoto de votantes presentan algunos retos de seguridad. Estos problemas se basan principalmente en la dificultad para verificar la identidad de una persona que desea registrarse en el censo electoral, y pueden facilitar la usurpación de identidades o la creación de múltiples registros por votante usando diferentes datos para cada uno de esos registros. Un ejemplo de este hecho se muestra en [El07].

En este capítulo se analizan los sistemas actuales de registro remoto de votantes y se propone un esquema en el cuál se combinan técnicas criptográficas con medidas biométricas para proteger la integridad del censo electoral. Algunos sistemas biométricos han sido considerados por diferentes propuestas para ser utilizados en la fase de votación [Ho07], sin embargo, ciertas características biométricas no han sido aprovechadas para el registro remoto de votantes.

5.2 Sistemas actuales de registro remoto de votantes

En algunos países como los Estados Unidos [Fv06] o el Reino Unido [El08] se utilizan sistemas de registro remoto de votantes. Los métodos utilizados por lo general permiten al votante rellenar, de manera remota, un formulario con sus datos personales y posteriormente enviar dicho formulario a una oficina de registro. Los formularios de registro son usualmente enviados al votante a través de correo postal u otro servicio de envío o bien, son descargados desde algún sitio de Internet y entonces son impresos para ser rellenados a mano. En cualquiera de estos casos, el votante rellena el formulario, lo firma y lo devuelve a los oficiales de registro a través de un servicio postal o cualquier otro canal de comunicación alternativo como fax o correo electrónico (en este caso adjuntando el formulario como un fichero escaneado) [Fv06]. Además, hay países [DoD06] en los que se está introduciendo el uso de interfaces remotas para permitir a los votantes rellenar el formulario de registro a través de Internet, agilizando de esta manera la adquisición remota de la información de registro de los votantes. Una vez que el formulario de registro ha sido enviado a través de ese medio, el votante puede verificar si

la información ha sido recibida por los oficiales de registro. Esto lo puede hacer contactando a dichos oficiales a través del teléfono o de correo electrónico.

En los casos previamente descritos, la identificación del votante se puede llevar a cabo a través de la verificación de información personal o bien, mediante la verificación de alguna característica biométrica del votante. En el primer caso, un oficial de registro verifica que el formulario contiene de manera correcta algún dato distintivo del votante. Dicho dato se encuentra previamente almacenado en una base de datos. Ejemplo de esto podría ser la fecha de nacimiento del votante, su número de seguridad social, etc. El problema de este tipo de identificación es que aunque aún cuando el dato a verificar se puede considerar privado, alguna persona cercana al votante puede conocerlo y por lo tanto usurpar la identidad del votante para llevar a cabo un registro ilegítimo. El segundo caso de identificación consiste en verificar alguna característica personal del votante, tal como la firma manuscrita sobre el formulario de registro o la huella dactilar. La autoridad de registro debería tener previamente almacenada dicha información del votante y entonces podría ser comparada con la recibida en el formulario de registro.

Entre las técnicas descritas, el uso de la firma manuscrita es la más usada en el registro remoto de votantes. Sin embargo, no suele usarse para la verificación del votante durante esta fase, ya que en muchos de los casos la autoridad de registro no cuenta con una base de datos de las firmas de los votantes previamente almacenada. La firma contenida en el formulario de registro es solamente utilizada para crear una base de datos de firmas que será usada para identificar a los votantes durante la fase de votación. Por ejemplo, en el caso de voto postal, la firma del votante almacenada durante el proceso de registro es comparada con la firma contenida en el sobre que contiene el voto para validar si el voto ha sido enviado por el votante legítimo. La precisión en la verificación de la identidad del votante se basa en la habilidad de los oficiales de registro al comparar las firmas. Si consideramos que dichos oficiales de registro no son expertos en reconocimiento de firmas, no se puede esperar tener un alto grado de precisión. Por otro lado, los actuales sistemas de registro remoto no verifican si una persona lleva a cabo dos o más registros usando datos de diferentes votantes legítimos, ya que el votante usará firmas diferentes.

Existen otros problemas en el registro remoto de votantes además de los ya mencionados con la identificación. Por ejemplo, la información del formulario de registro puede ser alterada después de que ha sido enviada por el votante. Además, la firma contenida en un formulario puede ser reutilizada por un atacante para enviar un formulario diferente con esa firma. Estos problemas se basan en el hecho de que la firma manuscrita es independiente del contenido del formulario. Algún cambio en el formulario, o la reutilización de la firma para otro formulario no pueden ser detectados simplemente verificando la firma.

Se puede resumir que los sistemas actuales de registro remoto de votantes presentan los siguientes desafíos:

- Precisión para validar la identidad del votante.
- Prevención de múltiples registros por votante.
- Integridad de la información del registro del votante.

A continuación se analizan las mejoras que puede ofrecer un sistema de registro remoto de votantes usando la combinación de técnicas criptográficas y biométricas.

5.3 Precisión de los sistemas biométricos

De alguna manera los sistemas de registro de votantes descritos anteriormente se basan en el uso de biometría. Los oficiales de registro usualmente verifican alguna característica intrínseca al votante que le identifica de manera única, por ejemplo una identificación con fotografía (reconocimiento facial) o una firma manuscrita (caligrafía). Sin embargo, la precisión en la identificación de tales características personales se dificulta si

consideramos que los oficiales de registro no son expertos en reconocimiento de características biométricas.

Los sistemas biométricos se especializan en la identificación de usuarios a partir del procesamiento de características únicas, ya sea físicas o de comportamiento. Dichos sistemas se clasifican en base a la característica del usuario utilizada para llevar a cabo la identificación, por ejemplo el ADN, huella dactilar, iris, retina, escritura, voz, etc. Sin embargo, la precisión en los diferentes sistemas biométricos es variada y cada uno de ellos presenta ventajas y desventajas.

Para que un sistema biométrico sea fiable, debe cumplir con los siguientes requisitos [JRP04]:

- *Universalidad*. Todos los usuarios deben poseer la característica biométrica en la que se basa la identificación.
- *Unicidad*. La característica debe distinguir a cada individuo de forma única.
- *Permanencia*. La característica biométrica debe permanecer en el individuo con el paso del tiempo.
- *Obtención*. El sistema biométrico debe proporcionar un medio o interfaz para obtener la característica fácilmente.
- *Rendimiento*. Se refiere a la rapidez y precisión en la identificación a través de la característica biométrica, así como a los recursos requeridos para llevar a cabo dicha identificación.
- *Aceptación*. Indica el nivel de aceptación entre las personas que deben aportar su característica biométrica para llevar a cabo la identificación.
- *Robustez*. Este requisito refleja el nivel de resistencia contra métodos fraudulentos que traten de engañar al sistema biométrico.

En el caso de un sistema de registro remoto de votantes debemos considerar un requisito adicional: el sistema biométrico debe estar disponible remotamente para la mayoría de los votantes hacia los que está dirigido el uso del sistema. Por lo tanto, la adquisición de la

información biométrica debe ser llevada a cabo utilizando medios o dispositivos estándares que estén al alcance de los votantes remotos. Esta restricción reduce el número de candidatos a las características de firmas manuscritas y de voz. La firma manuscrita puede ser adquirida remotamente a través de la digitalización (escaneo) del formulario de registro en donde se incluye la firma del votante. Por su parte, la voz puede ser adquirida remotamente a través de un teléfono estándar.

En el campo de la biometría de caligrafía, del cuál forma parte la firma manuscrita, existen dos técnicas de adquisición: escritura en línea (online) y escritura fuera de línea (off-line). La adquisición de la firma en línea toma en cuenta, además de los rasgos de la firma, otros aspectos como el tiempo que se emplea para hacerla, la presión que se ejerce al escribirla, la trayectoria de los trazos, etc. Sin embargo, la firma en línea no es una opción viable en el registro remoto de votantes ya que requiere que el votante cuente con un panel de escritura digital para poder introducirla. Por esta razón, el enfoque se centrará en analizar la firma llevada a cabo fuera de línea.

Haciendo uso de análisis comparativos ya existentes de sistemas biométricos como en [JRP04, Ti06], y tomando como punto de referencia la huella dactilar, las características biométricas de interés para el sistema remoto de registro de votantes satisfacen los requisitos descritos previamente tal como se muestra en la tabla 5.1.

Tabla 5.1. Comparación de tres sistemas biométricos desde el punto de vista de requisitos generales
Nivel de cumplimiento B=bajo, M=mediano y A= alto.

Característica	**Universalidad**	**Unicidad**	**Permanencia**	**Obtención**	**Rendimiento**	**Aceptación**	**Robustez**
Huella dactilar	A	A	A	M	A	M	M
Firma fuera de línea	M	M	B	A	B	A	B
Voz	M	M	M	A	M	A	B

En base a la comparación mostrada en la tabla 5.1 podemos concluir que la firma fuera de línea y la biometría de voz no son tan eficientes como la huella dactilar. Sin embargo, la introducción de biometría de voz en un sistema de registro remoto de votantes podría mejorar los sistemas actuales basados en firmas manuscritas.

Otro aspecto importante de rendimiento en los sistemas biométricos es la precisión en el proceso de identificación. En la literatura se consideran tres parámetros que ayudan a determinar dicha precisión de una manera cuantitativa:

- *Tasa de falso rechazo* (FRR). Es el porcentaje de usuarios autorizados que tratan de acceder al sistema y éste los declara como no autorizados.
- *Tasa de falsa aceptación* (FAR). Es el porcentaje de intentos de accesos de usuarios no autorizados los cuáles el sistema acepta como autorizados.
- *Tasa de igualdad de error* (ERR). Es el punto en el cuál FRR y FAR son el mismo valor.

En la tabla 5.2 se muestra una comparativa adicional de los sistemas biométricos ya comparados en la tabla 5.1. En este caso se consideran los parámetros de precisión descritos previamente (FRR, FAR y ERR).

Tabla 5.2. Comparación de tres sistemas biométricos desde el punto de vista de precisión

Característica	FRR	FAR	EER	Referencias
Huella dactilar	2.2%	2.2%	2.2%	[Ca06]
Firma fuera de línea	10-30	10-30%	10-30%	[KSX04, YJX07]
Voz	5-10%	2-5%	6%	[Re05, PM04]

Tal como se puede observar en la tabla 5.2, la huella dactilar es nuevamente la característica biométrica mejor valorada. Sin embargo, tal como se explicará más adelante en la descripción de la propuesta, el uso de la huella dactilar en los sistemas de registro remoto de votantes no ofrece ninguna ventaja respecto a los sistemas usados

actualmente. Por otro lado, la biometría de voz ofrece mayor nivel de precisión que la firma llevada a cabo fuera de línea. Los valores de los parámetros de precisión en la biometría de voz mostrados en la tabla 5.2 han sido obtenidos usando una comunicación telefónica [Re05].

5.4 Prevención de registros múltiples con sistemas biométricos

Uno de los problemas detectados durante el estudio de los actuales sistemas de registro remoto de votantes es la falta de capacidad para detectar múltiples registros generados por el mismo votante. A fin de analizar cómo se podría mitigar este problema debemos considerar los dos contextos de operación implementados por los sistemas biométricos para la autenticación de usuarios: verificación e identificación.

- *Verificación.* En este contexto, el sistema verifica una identidad comparando la información biométrica que aporta el usuario con la información almacenada en una base de datos. Para llevar a cabo la comparación, el usuario proporciona al sistema un nombre de usuario o identificador único y su información biométrica. Entonces, el sistema consulta la información biométrica específica de ese usuario que se encuentra almacenada en la base de datos. El sistema lleva a cabo la comparación "*uno-a-uno*", es decir, de la información biométrica proporcionada por el votante con la correspondiente en la base de datos para dicho usuario. De esta forma es posible determinar si un usuario es quien dice ser.
- *Identificación.* En este contexto, el usuario no necesita un nombre de usuario o identificador. El usuario sólo proporciona su información biométrica y el sistema tiene que identificar si tal información corresponde a alguno de los registros almacenados en la base de datos. En este caso, se lleva a cabo una comparación de "*uno-a-n*".

En base a la operación de estos contextos de autenticación podemos deducir que los sistemas actuales de registro remoto de votantes utilizan solamente el de verificación. Los

oficiales de registro utilizan la información personal del votante para acceder directamente a la firma almacenada en la base de datos y llevar a cabo la comparación de las firmas. Sin embargo, con el uso de biometría en un contexto de identificación, la característica biométrica de un votante podría ser verificada contra todos los registros de la base de datos. De esta forma, en caso de que el mismo votante intente registrarse más de una vez utilizando diferente información personal, podría ser detectado. Por lo tanto, el uso de la biometría en el contexto de identificación puede prevenir múltiples registros por votante.

5.5 Vinculación de biometría y contenido

A fin de superar la facilidad que puede tener un atacante para manipular el contenido de un registro de votante o bien para separar dicho contenido del elemento de identificación del votante, es necesario generar un vínculo entre el contenido del registro y el elemento de identificación. Un método usado actualmente para proteger de manipulaciones la información digital es a través de la firma digital. Una firma digital protege la información y vincula dicha información con el autor de la misma. Sin embargo, las firmas digitales requieren de una infraestructura jerárquica de certificación y gestión, es decir, una PKI.

Hasta ahora se ha evaluado en que manera la biometría puede contribuir para llevar a cabo eficientemente un proceso de registro remoto de votantes. No obstante, la principal idea, tal como se ha explicado antes, es lograr un vínculo incorruptible del contenido de un registro de votante con un elemento de identificación, es decir, con la característica biométrica del votante que lleva a cabo el registro. En la propuesta descrita en la siguiente sección se toma ventaja de la posibilidad de crear dicho vínculo a través de la biometría para mejorar los actuales sistemas de registro remoto de votantes.

5.6 Esquema de registro remoto de votantes

El esquema descrito en esta sección permite llevar a cabo el registro remoto de votantes de una manera eficiente y segura. El esquema protege la integridad de la información de registro de los votantes vinculando dicha información con la identidad del votante correspondiente. Esto se logra con la combinación de técnicas biométricas y criptográficas que no requieren de una infraestructura de clave pública. El esquema consiste principalmente en la creación de una "firma digital biométrica" de la información de registro generada por un usuario que solicita su inclusión en un censo electoral. Esto significa que la firma digital biométrica puede dar al mismo tiempo autenticación e integridad al contenido.

El escenario principal para la aplicación del esquema propuesto es el registro de votantes a través de Internet y utilizando la voz como característica biométrica. La voz permite llevar a cabo la vinculación del contenido del registro con el autor de dicho contenido, es decir, con el votante. Tal como se muestra en la tabla 5.2, la voz presenta un alto nivel de precisión. Los errores que se pueden presentar en un sistema biométrico basado en voz se deben principalmente a interferencia en la comunicación o a problemas de afonía temporal del votante. Sin embargo, dichos problemas no son relevantes si consideramos que el período de registro de votantes tiene una duración de varios días o semanas. Además la voz, a diferencia de otras características biométricas, es resistente a ataques de replicación, tal como se explicará más adelante.

Por otro lado, el esquema propuesto es ideal para sustituir los sistemas actuales de registro remoto de votantes que utilizan la firma manuscrita del votante como parámetro de identificación.

Para llevar a cabo el proceso de registro en el esquema propuesto son necesarias cuatro entidades: un ciudadano (votante) que solicita su inclusión en el censo electoral, un módulo de registro, un módulo de validación y el oficial de registro. Las funciones de

cada una de estas entidades dentro del proceso de registro se describen brevemente a continuación:

- *Votante*. El votante provee sus datos personales a fin de generar la información de registro. El votante también colabora en la generación de una prueba de registro basada en su información biométrica y en la información de registro.
- *Módulo de registro*. Esta entidad es utilizada como interfaz para introducir la información de registro del votante y para generar una prueba de integridad de dicha información.
- *Módulo de validación*. La prueba de registro es generada en esta entidad. Dicha prueba se genera a partir de la información biométrica aportada por el votante durante el proceso de registro.
- *Oficial de registro*. El oficial de registro recibe la información de registro de los votantes y lleva a cabo algunos procesos de validación de dicha información.

El proceso de registro de votantes se lleva a cabo en tres fases principales:

- Fase 1: introducción de la información de registro de votante y protección de la integridad.
- Fase 2: generación de una prueba de registro.
- Fase 3: validación de la información de registro.

5.6.1 Introducción de la información de registro de votante y protección de la integridad

El votante accede al sitio Web del módulo de registro a través de un canal de comunicación cifrado, por ejemplo TLS. El sitio Web provee un formulario de registro que el votante debe rellenar con sus datos personales. Una vez que se ha completado el formulario de registro, el módulo de registro genera una prueba de integridad. Esta prueba de integridad es una función criptográfica unidireccional aplicada a la información de registro proveída por el votante. La prueba de integridad generada es representada en

un formato que pueda ser legible por el votante, por ejemplo en notación base-32 [RFC06]. También podrían ser usadas otras notaciones para representar la prueba de integridad de una manera legible, sin embargo, la notación base-32 posee características que facilitan la usabilidad al prevenir errores de interpretación. Por ejemplo, el número "0" no se incluye en la notación a fin de evitar una confusión entre dicho número y la letra "o".

La prueba de integridad es mostrada al votante a través del mismo medio de comunicación. La figura 5.1 muestra la interacción entre el votante y el modulo de registro para llevar a cabo el registro remoto y para generar la prueba de integridad de dicho registro.

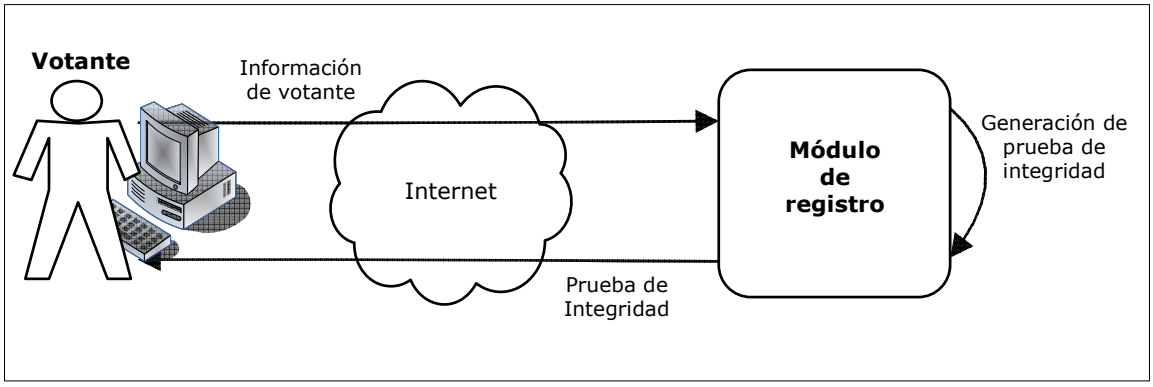

Figura 5.1. Interacción entre el votante y el módulo de registro

La prueba de integridad se genera utilizando una combinación de funciones hash MD5 y SHA1. La última de éstas es usada en su implementación MAC. La combinación de estas funciones es concebida con la idea de prevenir colisiones entre los resúmenes generados, tales como las encontradas en los últimos años para MD5 [Ha04, Kl05, Wa05, WY05] y para SHA1 [Wa05, WY05]. La generación de la prueba de integridad se lleva a cabo de la siguiente manera:

1. Se calcula un hash K de la información de registro M_i empleando una función MD5:

$$K_i = \text{MD5}\ [M_i]$$

2. Se utiliza K_i como clave para obtener un HMAC-SHA1 de la misma información de registro M_i :

$$H_i = \text{HMAC-SHA1}\ [M_i,\ K_i]$$

El valor resultante *H* es la prueba de integridad de la información de registro M_i.

Al emplear una combinación de las funciones MD5 y HMAC-SHA1 se disminuye significativamente la probabilidad de tener una colisión. Un atacante tendría que encontrar una coincidencia de colisión para el mismo mensaje en ambas funciones. Además, se reduce la probabilidad de dichas colisiones sin tener que incrementar el tamaño del , el cuál permanece igual que el del SHA1.

Debido a que *H* es el resultado de aplicar una función HMAC-SHA1, su longitud es de 160 bits, es decir, existen 2^{160} resúmenes diferentes. Por lo tanto, una notación base-32 permite la representación de un SHA1 en treinta y dos caracteres. Estos treinta y dos caracteres pueden ser mostrados al votante en ocho grupos de cuatro caracteres. Sin embargo, la prueba de integridad *H* puede ser truncada a fin de proporcionar una mayor facilidad de uso. Por ejemplo, si se consideran solo los primeros veinte caracteres, estos pueden ser mostrados en cinco grupos de cuatro caracteres, lo cuál es suficientemente usable para el votante.

A fin de prevenir ataques de replicación, cada formulario de registro tiene un número único de identificación, por lo cuál dos formularios con la misma información de registro tendrán diferentes pruebas de integridad.

Finalmente, el formulario con la información de registro de votante y la prueba de integridad son enviados al oficial de registro a través de Internet. La información de registro es almacenada por el oficial de registro para posteriormente ser validada, tal como se explicará más adelante.

5.6.2 Generación de la prueba de registro

La segunda fase del proceso de registro es la generación de una prueba de registro. Para la generación de la prueba de registro se utiliza la biometría de voz debido a las características ya mencionadas anteriormente. El votante establece una comunicación de voz con el módulo de validación. Dicha comunicación puede hacerse a través de la línea telefónica tradicional o bien, a través de sistemas VoIP. Una vez establecida la comunicación, el módulo de validación solicita al votante que pronuncie la prueba de integridad de su información de registro. El votante pronuncia la prueba de integridad que recibió previamente del módulo de registro, es decir, los grupos de caracteres que representan la prueba de integridad. Llevando a cabo este proceso, la voz del votante es vinculada al contenido de la información de registro. El resultado de dicha vinculación es lo que se denomina prueba de registro. La prueba de registro es almacenada por el módulo de validación. La figura 5.2 muestra la interacción que se lleva a cabo entre el votante y el módulo de validación a fin de generar la prueba de registro.

La prueba de registro protege la integridad de la información de registro. Cualquier manipulación en la información de registro causaría que la prueba de registro no corresponda al contenido de la información de registro. La prueba de registro también vincula el contenido de la información de registro al autor de la misma, es decir, al votante que provee su información personal.

La interacción entre el votante y el módulo de validación incluye, además de la pronunciación de la prueba de integridad, otros datos dinámicos a fin de prevenir ataques de replicación en los cuáles un atacante podría usar la voz del votante previamente grabada. Los datos dinámicos podrían consistir en uno o más retos en los que el votante debe repetir una palabra o una frase dicha por el módulo de validación. De esta forma, el módulo de validación puede asegurarse que la prueba de integridad está siendo pronunciada por el votante que se encuentra en el otro lado de la línea de comunicación, y no por una voz pregrabada o por un proceso automático. Esta característica que permite

evitar ataques de replicación no la tienen otros mecanismos biométricos. Por ejemplo en el caso de la huella dactilar, si un adversario lograra capturar la huella del votante, podría también responder a cualquier reto propuesto por el módulo de validación, ya que dichos retos sólo podrían consistir en colocar la huella en diferentes posiciones. Por lo tanto, el hecho de que el sistema basado en voz permita generar una diversidad de retos y que el responder apropiadamente a cualquier reto solamente se puede dar en el caso de que sea el votante legítimo el que está del otro lado de la comunicación, es una de las razones por las que se ha considerado que la voz es la mejor opción para el esquema propuesto.

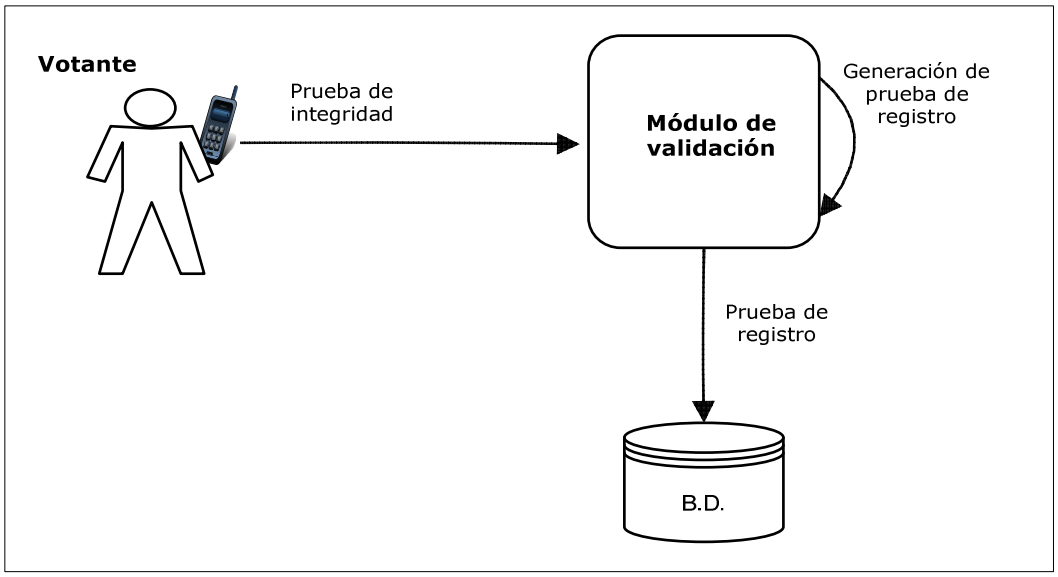

Figura 5.2. Generación de la prueba de registro

5.6.3 Validación de la información de registro

Con la información de registro del votante, la prueba de integridad de dicha información, y la prueba de registro, se pueden llevar a cabo diferentes validaciones a fin de detectar irregularidades en el proceso de registro remoto. A continuación se describen dichas validaciones:

- Detección de múltiples registros. Este proceso de validación facilita la detección de personas que intentan crear más de un registro. Es posible comparar la voz de un votante con el conjunto de voces registradas previamente. De esta forma, una persona que intenta crear un registro de votante adicional (y seguramente fraudulento) será detectada. En este caso, la información de registro asociada a la prueba proveída por dicha persona será identificada y marcada como inválida. Por lo tanto, la probabilidad de creación de múltiples registros por la misma persona es baja. Esta validación no es necesario llevarla a cabo en línea, sino que puede realizarse después del proceso de registro. Debido a que cualquier intento de crear registros fraudulentos puede ser detectado por medio del proceso de validación, el esquema no requiere una base de datos generada previamente con la voz de los votantes. Sin embargo, para procesos de registro futuros, los registros previos pueden ser usados para validar la voz de un votante que está llevando a cabo un nuevo registro.

- Correspondencia entre información de registro y prueba de registro. Otra validación que se puede llevar a cabo es la verificación de la correspondencia de la información de registro de un votante con la prueba de registro asociada. Esta validación consiste en verificar si la prueba de integridad proveída vocalmente por un votante concuerda con la prueba de integridad asociada a los datos de registro de dicho votante. Esto significa que se lleva a cabo una comparación del hash de la información de registro almacenada con la prueba de integridad que está proporcionando el votante. En el caso de que la prueba de integridad proveída por el votante no corresponda con la prueba de integridad del registro de información de dicho votante, se debería anular el almacenamiento de la prueba de registro o marcarlo con un estatus de "inválido".

Si la prueba de registro y la información de registro del votante pasan ambas validaciones, el oficial de registro puede clasificar la información de registro del votante con un estatus de "validada". Sin embargo, si alguna de las validaciones falla la información de registro del votante y su correspondiente prueba de registro pueden ser

clasificadas como inválidas. Por lo tanto, el oficial de registro puede implementar validaciones manuales adicionales o contactar a los votantes cuyos registros necesiten ser verificados más ampliamente.

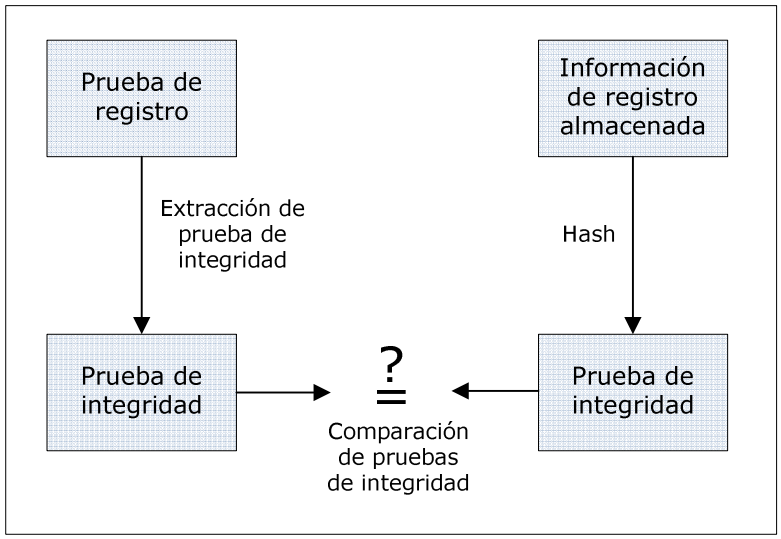

Figura 5.3. Validación de las pruebas de registro

En una subsiguiente fase de votación remota sería posible utilizar la prueba de registro para verificar que la persona que envía el voto es la misma que llevó a cabo el registro. Esto se lleva a cabo comparando la voz del votante con la voz almacenada en la fase de registro.

En la figura 5.4 se muestra, a manera de resumen, el proceso de registro remoto.

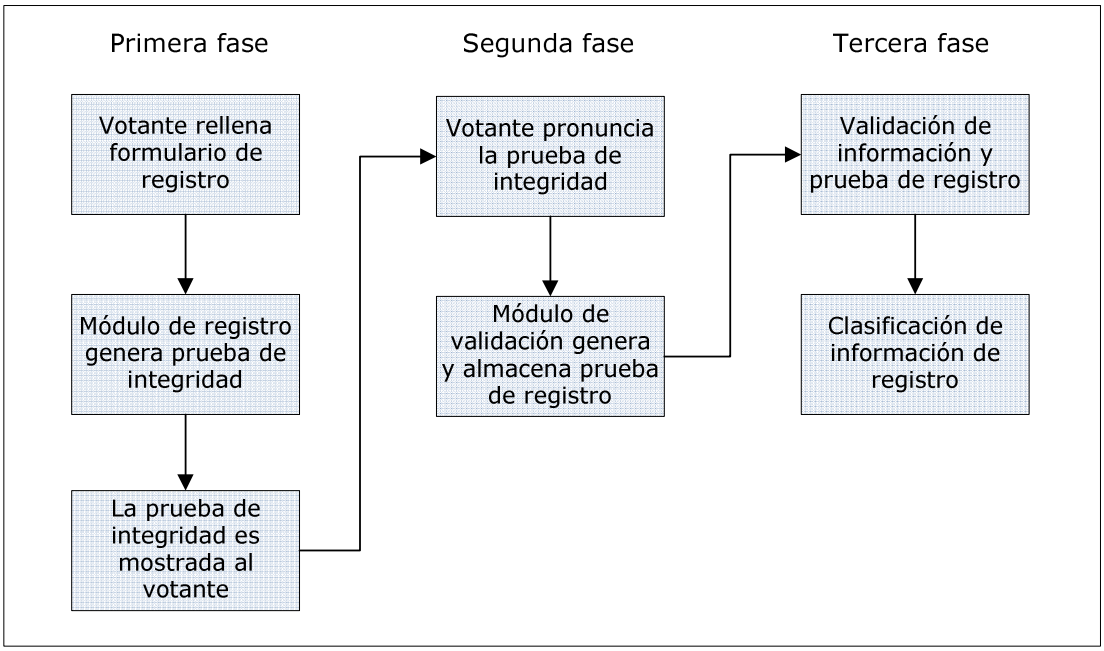

Figura 5.4. Proceso de registro remoto

5.6.4 Método alternativo para la generación de la prueba de registro

Otro método de generación de la prueba de registro es utilizando como parámetro biométrico la caligrafía del votante en lugar de la voz. El proceso de generación de la información de registro y prueba de integridad se lleva a cabo de la forma ya descrita en la sección 5.6.1. El proceso de generación de la prueba de registro se lleva a cabo a través de la escritura manual de la prueba de integridad por parte del votante. De esa forma, la prueba de registro vincula la información de registro con la caligrafía del votante. El votante escribe la prueba de integridad en un formulario proveído por la autoridad de registro. El formulario es entonces enviado por correo postal o a través de un medio electrónico, como fax o corro electrónico. En el caso de que el envío se realice a través de un medio electrónico, el formulario debe ser previamente digitalizado. Las validaciones de la información de registro se llevan a cabo de la forma ya descrita en la sección 5.6.3.

5.7 Conclusiones y aportación

Los sistemas actuales de registro de votantes tienen algunas deficiencias que pueden facilitar la usurpación de la identidad de votantes. Dichas deficiencias están relacionadas principalmente con la precisión en la identificación de los votantes, con la posibilidad de múltiples registros por votante y con la manipulación de la información de registro de un votante.

En este capítulo se ha propuesto un esquema que hace uso de sistemas biométricos para incrementar la precisión en la identificación de los votantes a través de medios remotos. Se ha presentado una solicitud de patente internacional de dicho esquema y de las implementaciones posibles [PMV07a]. Además, el esquema ha sido presentado y publicado en [MPS08].

Para llevar a cabo de manera segura el registro remoto, se ha elegido la voz del votante como sistema biométrico que permite vincular la información de registro con la identidad del votante. Además de presentar características que permiten llevar a cabo la vinculación del contenido del registro con el autor del mismo, un sistema basado en la voz posee otras características que son determinantes para la eficiencia del esquema propuesto. La voz es fácilmente obtenida por medio de dispositivos de comunicación estándar, como el teléfono. Por otro lado, al utilizar la voz del votante para generar la prueba de registro se evitan ataques en los que un adversario tenga pregrabada la voz del votante para usarla durante el proceso de registro. Esto se logra por medio de retos que requieren al votante pronunciar datos de manera dinámica.

De manera adicional, en un contexto de identificación los sistemas biométricos utilizados permiten automatizar la detección de múltiples registros realizados por la misma persona.

Capítulo 6

Verificación Individual

6.1 Introducción

Un sistema de voto electrónico puede considerarse fiable si cumple con algunos requerimientos de seguridad como privacidad y precisión, entre otros. Para preservar la precisión de los resultados de una elección no es suficiente contar con un sistema que lleve a cabo apropiadamente el registro y el escrutinio de los votos. Existen factores externos que podrían comprometer el contenido de los votos y por lo tanto, la precisión de los resultados de la elección. En [Ru01], se destacan potenciales riesgos de seguridad de los sistemas de voto electrónico remoto. La mayoría de los riesgos mencionados son la consecuencia de la inseguridad que se presenta en el entorno del votante, el cuál no es controlado por el sistema de votación. Ese entorno está compuesto por el terminal de votación y por el canal de comunicación entre dicho terminal y el servidor de votación.

En sistemas de voto convencionales basados en papel los votantes pueden verificar que su voto es recibido correctamente ya que son ellos mismos quienes colocan la papeleta en la urna física. Sin embargo, los votantes no pueden verificar que sus votos son parte del escrutinio.

Por su parte, los sistemas de voto electrónico remoto pueden proveer medios que permitan a los votantes verificar el correcto tratamiento de su voto durante el proceso de escrutinio, es decir, que el voto ha sido correctamente incluido. Si los votantes tienen la

oportunidad de verificar la inclusión de su voto en el escrutinio, la fiabilidad del sistema de votación incrementa considerablemente.

La verificación individual es un aspecto muy importante para validar el correcto funcionamiento de un sistema de voto electrónico remoto. El principal objetivo de la verificación individual es que el votante pueda estar seguro que su voto se ha registrado correctamente y que además su voto ha sido incluido en el escrutinio y publicación de resultados. Sin embargo, esta verificación no debería abrir la posibilidad de coerción o venta de votos. En consecuencia, un sistema de votación debería incluir mecanismos de verificación que permitan al votante tener la certeza de que su voto ha sido contabilizado sin que dicha verificación indique cuál ha sido la elección del votante.

Actualmente la mayoría de las propuestas que contemplan la verificación individual en los sistemas de voto electrónico están enfocadas al voto electrónico presencial, siendo complejo y en ocasiones imposible llevarlos a la práctica en un ambiente remoto de votación.

En este capítulo se describirán los sistemas de verificación individual propuestos a la fecha. Se analizará la eficiencia y factibilidad de estos sistemas y se presentarán dos propuestas de verificación individual para sistemas de voto electrónico remoto. La primera propuesta consiste en un recibo criptográfico de votación basado en una tarjeta inteligente. La segunda propuesta describe un sistema completo de voto electrónico remoto enfocado principalmente en proporcionar a los votantes algunos mecanismos que les permitan llevar a cabo la verificación del tratamiento de sus votos desde el momento en que los votos son emitidos hasta el tiempo de la publicación de los resultados.

6.2 Sistemas de verificación independiente

En el apéndice B del informe del “Voluntary Voting Systems Guidelines” [VVSG06] se describe una clasificación de métodos que podrían aplicarse tanto a la verificación del

votante como a la auditoria de los sistemas de votación. Estos métodos son conocidos como sistemas de verificación independiente. Dicha clasificación es la siguiente:

- Sistemas de verificación directa.
- Sistemas de procesos separados.
- Sistemas de testigos.
- Sistemas de verificación con cifrado extremo a extremo.

En base a las especificaciones descritas en dicho informe, los sistemas de verificación independiente tienen dos objetivos principales. Por un lado, permitir al votante verificar que su voto se ha registrado correctamente y, además, generar un registro independiente de los votos para que pueda ser usado en caso de auditoria.

Los sistemas de verificación independiente deben proteger la integridad de la elección contra daños ocasionados de manera accidental o premeditada, que podrían llegar a eliminar o alterar los votos emitidos por los votantes así como insertar votos ilegítimos.

Para lograr un nivel aceptable de verificación y auditoria, los sistemas de verificación independiente deben cumplir con las siguientes características:

- Además del registro que permanecerá almacenado en el sistema de votación para efectos del escrutinio, se debe generar otro registro con almacenamiento independiente. El segundo registro es creado a partir del propio sistema de voto, sin embargo es almacenado en un entorno independiente del mismo.
- El votante debe tener la posibilidad de verificar que ambos registros coincidan con su selección de voto.
- Ambos registros deben contar con un identificador común de tal manera que se puedan relacionar si se efectúa una auditoria.

De acuerdo a lo descrito en los puntos anteriores, y como resultado de la independencia entre registros, uno de ellos puede ser usado para auditar o para verificar la integridad del

otro. Por otro lado, un atacante que logre alterar un registro de voto, todavía tendría que alterar el segundo registro para que su ataque sea exitoso.

A continuación se muestra una descripción detallada de cada uno de los sistemas de verificación independiente propuestos en [VVSG06].

6.2.1 Sistemas de verificación directa

Los sistemas de verificación directa pretenden generar y almacenar un segundo registro del voto equivalente al original en contenido pero en un tipo de almacenamiento distinto. Básicamente el segundo registro, o registro de respaldo, es un registro impreso en papel. Tal registro físico debe contener la selección hecha por el votante y puede ser directamente leído por percepción humana, es decir, que no se requiere de algún dispositivo especial para leer o interpretar su contenido.

Dentro de esta categoría existen algunas propuestas basadas en el reconocimiento óptico de marcas que generan tanto una versión impresa del voto como una electrónica. Además, dentro de esta clasificación existen los sistemas "VVPAT" (Voter Verified Paper Audit Trail) propuestos por Rebeca Mercuri [Me02], los cuáles son una extensión a las plataformas de Registro Electrónico Directo.

En los sistemas de verificación directa, por ejemplo los de reconocimiento óptico de marcas, el votante escoge e imprime su voto a través de una máquina de voto. A continuación, el votante verifica que la papeleta impresa corresponde a su selección. Esta papeleta se coloca en un escáner de reconocimiento de imágenes y dicho escáner genera un registro electrónico de la papeleta. La papeleta impresa se coloca en una urna física y el registro electrónico del voto es almacenado en una base de datos.

Un sistema VVPAT es similar al descrito anteriormente, sin embargo, los sistemas VVPAT se componen de un terminal DRE que crea y almacena un registro electrónico y de una impresora que genera el registro físico de los votos. El votante verifica que el

registro impreso corresponde con las opciones seleccionadas. Por último, una vez que el votante valida la verificación, el registro impreso se coloca en una urna física. El votante, aún pudiendo ver el registro impreso, no puede manipularlo ya que éste se encuentra detrás de un cristal para prevenir alteraciones.

En las dos propuestas descritas anteriormente se genera un registro paralelo en donde el votante, a simple vista, puede constatar que su voto se ha registrado correctamente. Ejemplos de sistemas de verificación directa se incluyen en las siguientes propuestas:

- Con la finalidad de prevenir problemas de privacidad, David Chaum propuso un sistema de votación electrónica que genera un recibo de votación protegido con técnicas de criptografía visual [Ch04]. En esta propuesta el voto es emitido a través de un terminal de votación. Una vez que el votante ha escogido sus opciones se imprime el recibo de votación, compuesto de dos hojas transparentes que contienen pixeles y que por sí solos no representan nada. Cuando este par de hojas son colocadas de manera alineada una encima de la otra se forma una imagen que revela al candidato elegido por el votante. El votante se queda con una parte del recibo y entrega la otra parte a la autoridad local de la elección para que sea destruida. Por otra parte, el terminal de votación almacena la versión electrónica de la parte que el votante ha elegido conservar. Al final de la elección, el votante puede verificar en una página Web de la elección que la parte del recibo que el posee es idéntica a la parte electrónica del recibo que está publicada. De esta manera se asegura que su voto se ha tenido en cuenta.

- Ryan [Ry04] llevó a cabo una revisión de la propuesta de Chaum y propuso algunas mejoras que facilitan su implementación. Esta propuesta conserva muchas de las características de la propuesta anterior, sin embargo elimina la criptografía visual del recibo de Chaum. En su lugar propone que los candidatos sean presentados al votante en un orden aleatorio. Los candidatos se muestran alineados en una columna, y en otra columna el votante debe marcar su voto. Entonces el votante escoge una de las dos columnas para conservarla como

recibo. Se imprime entonces la papeleta en donde al final de cada columna se especifica si esa columna debe ser conservada por el votante o entregada a la autoridad de la elección para que sea destruida. El votante separa ambas columnas, conserva la columna elegida y entrega la otra a la autoridad. Cuando el votante elige la columna que desea como recibo, el terminal de voto almacena esa misma columna. En la publicación de los resultados el votante podrá verificar que su recibo aparece publicado, y por lo tanto que su voto se ha incluido en el escrutinio de votos.

Además de los ya descritos, se pueden consultar otros esquemas que incluyen un sistema de verificación directa en [CRS04, FCS06 y Ri06a].

Las propuestas descritas previamente para sistemas de verificación directa requieren de una urna física en donde los registros puedan ser protegidos de manipulación. Esta tarea evidentemente no es aplicable a los esquemas de voto electrónico remoto, por lo que su uso se restringe a los entornos de voto electrónico presencial.

6.2.2 Sistemas de procesos separados

Los sistemas de procesos separados se componen de dos sistemas independientes. Se cuenta además con un dispositivo de almacenamiento portátil o Token. Uno de los sistemas contiene la plataforma que permite al votante seleccionar su voto y grabarlo en el dispositivo de almacenamiento. El segundo sistema se encarga de ejecutar los procesos de verificación. Este sistema es capaz de leer el contenido almacenado en el dispositivo de almacenamiento. Además hace una copia de las opciones elegidas por el votante y las despliega para que el votante pueda visualizarlo y verificar que concuerdan con su selección. Una vez que el votante confirma que la información desplegada por el segundo sistema corresponde a la seleccionada en el primer sistema, el dispositivo de almacenamiento es colocado en una urna física. Se conservará como registro de votación tanto lo desplegado por el sistema de verificación como el registro contenido en el

dispositivo de almacenamiento. Cualquiera de los dos registros deberá estar disponible para llevar a cabo el escrutinio de los votos.

Este tipo de sistemas requieren el uso de un segundo sistema que permita la verificación y almacenamiento, y por ello resultan poco flexibles para entornos de voto electrónico remoto.

6.2.3 Sistemas de testigo

Un sistema de testigo también permite llevar a cabo un segundo registro del voto. Esto se realiza por medio de un módulo separado que registre en tiempo real, es decir, durante la elección del voto, las opciones escogidas por el votante. El registro secundario podría ser una imagen de la pantalla en donde se muestran las opciones del votante una vez que estas han sido confirmadas. Esa imagen puede ser captada con una cámara habilitada frente a la pantalla de votación. Otra posible aplicación de sistema de testigos podría ser una grabación de audio de las opciones elegidas por el votante. Esto se lograría usando un sistema de votación en el cuál se tenga una interfaz con salida de audio. De esta manera, además de mostrar las pantallas de votación de manera visual, se presenta el proceso de una manera audible. Al mostrar al votante la pantalla de confirmación también se dispondría del audio describiendo el resumen de las opciones elegidas por el votante, lo cuál sería grabado de manera independiente. La grabación de audio tiene una ventaja sobre el resto de sistemas de verificación: permite que los votantes con discapacidad visual o problemas de lectura puedan saber el resumen de los votos escogidos al escuchar la grabación.

El problema común de los sistemas de verificación independiente descritos arriba (verificación directa, procesos separados y sistemas de testigo) es que si se detecta alguna discrepancia entre ambos grupos de registros (el almacenado por el sistema de voto, y el almacenado de manera independiente) es difícil determinar cuál de ellos es el válido. Por lo tanto, aunque es posible detectar cuando los resultados de una elección han sido alterados, no es fácil determinar cuál de los registros es el correcto.

Por otro lado el uso de estos sistemas de verificación independiente está limitado a los entornos de voto electrónico presencial. En un ambiente de votación remota es aún más difícil permitir la verificación por parte del votante del correcto tratamiento de su voto. Como ya se ha mencionado antes, la mayoría de las soluciones de verificación propuestas a la fecha están enfocadas principalmente al voto electrónico presencial, siendo difícil llevar a cabo su implementación en entornos de voto electrónico remoto.

6.2.4 Sistemas de verificación con cifrado extremo a extremo

Los sistemas de verificación con cifrado extremo a extremo fueron clasificados por la "Voluntary Voting Systems Guidelines" [VVSG06] como sistemas de verificación independiente, y originalmente fueron propuestos para entornos de voto presencial. Sin embargo, a diferencia de los tres sistemas de verificación independiente descritos previamente, estos sistemas poseen características que les permiten ser implementados en entornos de votación remota.

Los sistemas de verificación con cifrado extremo a extremo, también llamados sistemas basados en recibos de votación, utilizan técnicas criptográficas para generar un recibo de votación. Los recibos de votación permiten a los votantes verificar el correcto tratamiento de su voto. Es decir, por medio del recibo de votación el votante puede verificar que su voto ha sido incluido en el escrutinio final y en caso de detectar que su voto no se ha contabilizado, el votante cuenta con un recibo que le permite reclamar ante la autoridad correspondiente.

La emisión de recibos de voto puede abrir la posibilidad de coerción o venta de votos si el recibo revela el contenido del voto elegido por el votante. Por lo tanto un recibo de voto debe permitir que el votante verifique que su voto se ha incluido en el escrutinio, pero no debe revelar el contenido del mismo.

En general, un recibo de votación debe cumplir con las siguientes características de seguridad [PM07a]:

- *Resistencia a manipulaciones*. Los recibos de votación deben ser resistentes a manipulaciones. por parte del votante y de terceros, incluyendo las autoridades de la elección. Por lo tanto, nadie debe tener la posibilidad de alterar el contenido de un recibo de voto sin que esta acción sea detectada.

- *No repudio*. Los votantes y las autoridades de la elección deben poder verificar la autenticidad del recibo de votación. Una vez emitido el recibo, la autoridad no debe poder negar que este es un recibo emitido por ella y por lo tanto un recibo de votación válido. Por otro lado, una vez recibido por el votante, éste no debe poder negar que lo ha recibido y que corresponde al voto que previamente ha enviado.

- *Prevención de recibos falsos*. La autoridad electoral y los votantes solamente deben poder generar recibos de votación que correspondan a un voto emitido por un votante legítimo. No debe ser posible generar recibos que no tengan relación con un voto y en caso que se generen, debería ser detectado fácilmente.

Se han propuesto algunos esquemas que incluyen un recibo de votación. A continuación se describen algunos de esas propuestas.

En [CC97] se propuso un recibo de votación simple: se trataba únicamente del voto cifrado y firmado por una autoridad de la elección. La principal desventaja de esta propuesta es que si el votante reclama la ausencia de su voto en el escrutinio final, se debería descifrar el contenido del voto para poder comprobarlo. Por lo tanto, este esquema viola la privacidad del votante cuando se dan esas circunstancias.

Por su parte, Sako [Sa94] propuso que el votante genere un par de claves (pública y privada) durante la fase de votación. La clave privada generada la utiliza para firmar digitalmente el voto. La clave pública es firmada ciegamente por una autoridad de

validación. El voto digitalmente firmado y la firma digital de la clave pública son entonces enviados a la autoridad colectora de los votos. Una vez que el voto ha sido aceptado, la autoridad colectora firma digitalmente la clave pública generada por el votante y se la devuelve. El resultado de esta firma es entonces el recibo de votación. La verificación por parte del votante consiste en comprobar que en la lista de resultados existe un voto que ha sido firmado digitalmente con su clave privada. Si surge un problema entonces el votante puede reclamar mostrando su clave pública, la cuál ha sido firmada digitalmente por la autoridad colectora, para demostrar que su voto fue enviado y recibido. Este recibo presenta algunos problemas. Por ejemplo, el rendimiento del proceso, ya que la generación de claves asimétricas requiere un costo computacional considerable. Por otro lado, para evitar que los votantes generen recibos falsos, el proceso de firma ciega por parte de la autoridad de validación debería complementarse con la implementación de alguna técnica de corte y elección, tal como las descritas por Schneier [Sc96]. Estas técnicas comprenden la generación de un conjunto de *n* mensajes (en este caso pares de claves) suficientemente grande que deben ser enviados a la autoridad de validación para realizar una comprobación de que el mensaje a firmar ciegamente no es malicioso. Al recibir el conjunto *n* de claves públicas, la autoridad de validación escoge *n-1* claves para las cuáles debe ser revelado el factor de cegado. La autoridad entonces recupera las *n-1* claves y verifica su integridad. Una vez validados, si no se han detectado irregularidades, la autoridad de validación firma ciegamente la única clave restante y la envía al votante. Por lo tanto, llevar a cabo este proceso implica la generación de un conjunto grande de pares de claves, lo cuál es totalmente impráctico.

Riera y otros [RRB00] describieron un recibo de votación que consiste en la aplicación de una función hash sobre la concatenación del voto y una cadena de relleno aleatoria. Este valor hash es firmado ciegamente por la autoridad, tal como en el esquema de Sako [Sa94], y de la misma manera, se utiliza alguna técnica de corte y elección para validar la información antes de firmarla. Aún cuando en éste esquema la generación de *n* mensajes es mucho más rápida debido al bajo coste computacional para generar resúmenes, el problema de rendimiento permanece.

En términos generales, un recibo de votación criptográfico, como los ya descritos, permite la verificación del escrutinio correcto, es decir, que el votante puede verificar que el voto que se incluyó en el escrutinio es el mismo que la autoridad de la elección recibió. Por lo tanto, por medio de una implementación correcta de un recibo de votación criptográfico se protege la integridad del voto desde el momento en que la autoridad lo recibe, hasta el momento que se lleva a cabo el escrutinio. Sin embargo, esta verificación no es del todo fiable, ya que los votantes no pueden verificar que el voto almacenado en el servidor de votación y posteriormente contado es realmente la intención del votante. Esto se debe a que el terminal de votación es propenso a ataques (por ejemplo software malicioso) que pueden cambiar dicha intención del votante antes de que el voto sea protegido por medio de criptografía. Por lo tanto, los recibos de votación por sí solos no satisfacen la verificación del registro correcto del voto en el servidor de votación.

6.3 Otros mecanismos de verificación

Además de los sistemas de verificación independiente descritos en la sección anterior se han propuesto otros mecanismos que dan a los votantes la posibilidad de verificar el tratamiento de sus votos. Estos mecanismos serán descritos a continuación.

6.3.1 Verificación con esquemas de papeletas precifradas

Uno de los propósitos de las papeletas precifradas es proporcionar a los votantes un medio para llevar a cabo la verificación del registro correcto de sus votos, lo cuál, como hemos visto en este capítulo no ha sido resuelto mediante un recibo criptográfico de votación. Los esquemas de papeletas precifradas ya han sido descritos ampliamente en el capítulo 4. En esta sección sólo se incidirá en la manera en que estos esquemas favorecen la verificación por parte de los votantes y por otro lado se hará hincapié en los riesgos y problemas de seguridad asociados a dichos esquemas.

En algunos de los esquemas de papeletas precifradas, la propia papeleta precifrada se puede considerar también como un recibo de votación preimpreso. En estos esquemas se permite al votante llevar a cabo la verificación de que su voto ha sido recibido correctamente por la autoridad de la elección (registro correcto). Tales esquemas incluyen en la papeleta precifrada, además del código de votación, un código de verificación para cada código de votación. Entonces, durante la fase de voto, cuando el votante envía un código de votación, deberá recibir de la autoridad de votación el código respuesta que corresponde al candidato elegido, tal como está escrito en su papeleta. Por lo tanto, el votante puede comprobar que su voto ha sido recibido correctamente por la autoridad de la elección. En este sentido, la papeleta precifrada sirve como recibo de votación durante esta fase. En la figura 6.1 se muestra el proceso llevado a cabo en una sesión de voto.

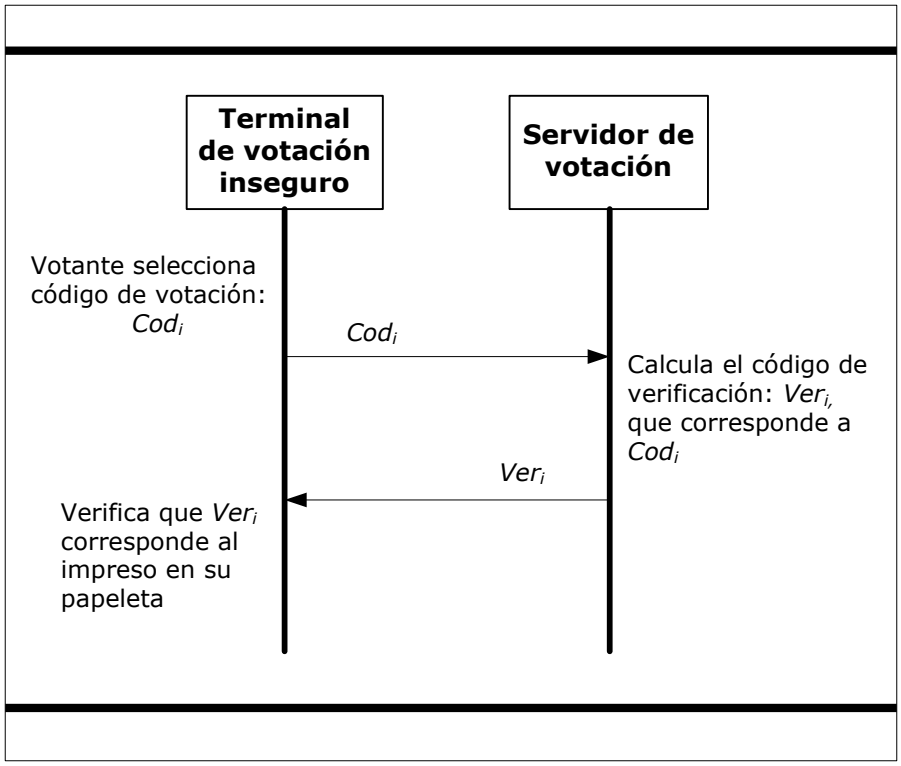

Figura 6.1 Proceso de votación con un esquema de papeletas precifradas

Los esquemas de papeletas precifradas proporcionan una gran ventaja de verificación, sin embargo, los desafíos de seguridad que presentan pueden ser una razón fundamental para

no llevar a cabo la implementación de esquemas de este tipo. Se pueden destacar tres problemas principales:

- *Manipulación de las papeletas*. Las papeletas impresas son propensas a manipulación en el intervalo entre su generación y la entrega de las mismas a los votantes. En un esquema en dónde no se utilizan códigos de verificación, alguien podría simplemente modificar la relación de códigos y candidatos impresos en las papeletas en base a algún criterio que favorezca a los intereses del autor del ataque. Por su parte, en un esquema que utilice códigos de verificación, el atacante puede cambiar la relación de los pares de códigos (código de votación y su código de verificación) con sus candidatos asignados. Si el votante no nota el cambio en la papeleta, enviará un voto diferente al deseado sin percatarse de ello debido a que el votante recibirá como respuesta el código de verificación correspondiente al código de votación enviado. Un ejemplo de este ataque se muestra en la figura 6.2. Desde luego el éxito de un ataque como el descrito dependerá de otros factores. Para que el atacante esté seguro de que la manipulación de la papeleta beneficiará sus intereses, se debe tener un conocimiento previo de la intención de voto del votante. En este sentido, el ataque debería ser cuidadosamente selectivo. En elecciones con tres o más candidatos existe una forma de beneficiar a un candidato específico a través de la manipulación de las papeletas. El atacante intercambia los códigos del principal oponente con uno o más de los candidatos minoritarios. De esta forma, el principal oponente perderá votos y el candidato favorecido obtendrá una ventaja. En cualquier caso, las medidas de seguridad empleadas durante la generación y distribución de las papeletas precifradas afectarán el éxito de estos ataques.

- *Privacidad*. Un atacante que tiene acceso a una papeleta precifrada podría comprometer la privacidad del votante al relacionar el voto con el votante que lo envía. Sin embargo, para llevar a cabo este ataque deberían presentarse condiciones particulares. El atacante debería tener acceso a los siguientes elementos:

- Papeleta precifrada. El acceso a la papeleta precifrada puede darse en dos diferentes contextos: a) durante la generación y distribución de las papeletas o b) en el propio entorno del votante.
- Servidor de votación. El acceso al servidor de votación puede llevarse a cabo en dos formas: a) a través de la colaboración de la autoridad de la elección a cargo del servidor de votación o b) a través del personal técnico con privilegios de acceso.

Sin embargo, para llevar a cabo este tipo de ataques se tiene que asumir que no existen medidas de control de acceso adecuadas. La violación de la privacidad de un votante también puede llevarse a cabo si se logra acceso a la papeleta precifrada y además se logra capturar el código de votación durante su transmisión desde el terminal de votación hacia el servidor.

- *Coerción o venta de votos*. Los sistemas de votación basados en papeletas precifradas presentan un riesgo de coerción o venta de votos, como todos los sistemas de voto remoto. Sin embargo, con un esquema de papeletas precifradas este riesgo se incrementa si los códigos de votación recibidos por el servidor de votación son publicados o si el atacante logra el acceso a esa información por otros medios.

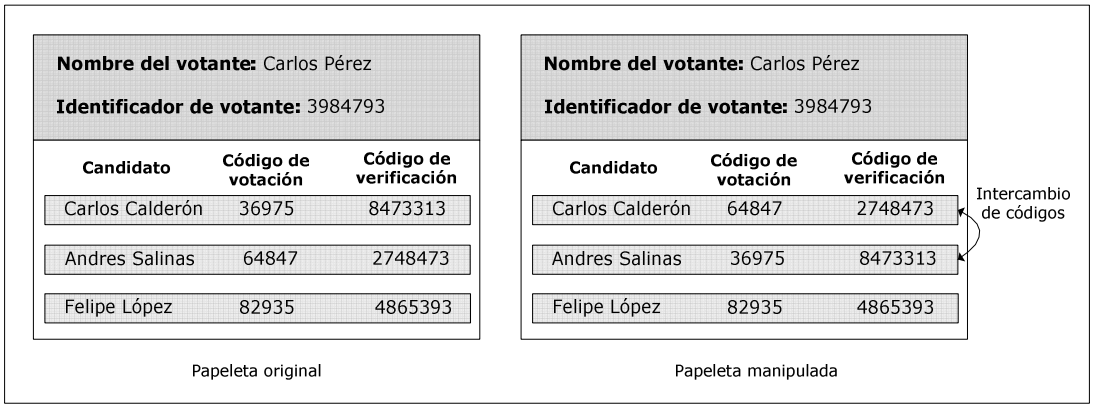

Figura 6.2. Ataque de manipulación de la papeleta

Adicionalmente, se puede presentar cierta reticencia a un sistema de votación basado en papeletas precifradas debido a aspectos de usabilidad. En los sistemas convencionales de voto electrónico el votante usualmente escoge un candidato seleccionando el nombre o fotografía de dicho candidato. Por su parte, con un esquema de papeletas precifradas, el votante debe teclear el código que corresponde al candidato elegido. Esta situación podría resultar compleja o incómoda para algunos votantes. Sin embargo, un estudio de usabilidad de dichos esquemas ha mostrado un buen nivel de aceptación entre votantes en general [SLD06].

6.3.2 Tablón de anuncios electrónico

Otro mecanismo de verificación en un entorno de voto electrónico remoto ha sido propuesto con la implementación de un tablón de anuncios electrónico público (public electronic bulletin board o EBB). En dicho tablón de anuncios se reciben y se hacen públicos los votos que se van recibiendo (generalmente cifrados) durante la fase de votación y se mantienen publicados aún después del cierre de la fase de votación para mostrar la lista de votos recibidos y contados.

Los votos cifrados publicados en el tablón de anuncios electrónico usualmente se muestran junto con un identificador único o con una prueba de la identidad del votante. De esta forma, el votante puede verificar que su voto cifrado aparece en el tablón de anuncios y por lo tanto que ha sido recibido correctamente.

Al final de la elección, el votante puede verificar también que su voto aparece en la lista de votos contados. Sin embargo, el votante no puede estar seguro que su voto ha sido contado correctamente, es decir, no tiene la posibilidad de verificar que su voto se descifró correctamente y permaneció sin alteración hasta el proceso de escrutinio.

Por otro lado, ya que los votos publicados en el tablón de anuncios contienen un identificador que lo relaciona con el votante, un adversario podría llevar a cabo un ataque de coerción como el descrito por Juels y Jakobsson [JJ02]. Este ataque consiste en forzar

a un votante, cuya preferencia de voto se conoce de antemano, a que se abstenga de emitir su voto. El atacante podría verificar que realmente dichas personas no han emitido su voto, ya que su identificador no consta en el tablón de anuncios. Por medio de este ataque se puede dar ventaja a un candidato específico.

6.4 Propuesta de verificación: recibo de votación con tarjeta inteligente

Como se ha mencionado al inicio de este capítulo, en un sistema de voto electrónico remoto es muy importante que el votante tenga la oportunidad de verificar que su voto ha sido incluido en el escrutinio de los votos. El lograr este hecho permite aumentar la confianza de los votantes en un sistema de votación.

En esta sección se describirá un recibo de votación que se genera por medio de una tarjeta de votación como la utilizada en el esquema de votación propuesto en [MSM+08] y descrito en el capítulo 3 de esta tesis. Dicha tarjeta de votación es una tarjeta inteligente de red protegida por un número de identificación personal y por la huella dactilar del votante. Estos elementos de identificación son requeridos en la fase de votación para llevar a cabo la identificación del votante y de igual manera son requeridos para la verificación del voto.

La tarjeta de votación es utilizada para la generación de un recibo criptográfico de votación, así como para el almacenamiento del mismo. El recibo de votación propuesto permite al votante verificar que su voto ha sido incluido en el escrutinio sin que dicho recibo revele el contenido del voto. Este recibo de votación es generado y almacenado en la tarjeta de votación durante la sesión de voto, tal como será explicado más adelante. De esa forma sólo el votante legítimo, portando su tarjeta de votación, puede verificar la inclusión de su voto en los resultados.

El recibo de votación propuesto puede ser adaptado a diferentes esquemas de voto electrónico, sin embargo la siguiente descripción del recibo está basada en la adaptación del mismo al esquema de votación descrito en el capítulo 3.

6.4.1 Generación del recibo de votación

El recibo de votación es un código alfanumérico cifrado con una clave aleatoria generada en la propia tarjeta de votación. Por lo tanto, para llevar a cabo la generación del recibo, la tarjeta de votación debe contener un generador de claves aleatorias. La generación del recibo se lleva a cabo con la participación de la tarjeta del votante y del servidor de votación, tal como se describe a continuación.

Durante la fase de votación se llevan a cabo los siguientes pasos en cada sesión de votante:

1. La tarjeta de votación genera de forma aleatoria una clave simétrica g.

2. La clave g es cifrada con la clave pública del servidor de votación.

3. La clave g se adjunta al mensaje que contiene el voto cifrado y se envía al servidor de votación.

4. El servidor de votación descifra la clave simétrica g.

5. El servidor de votación genera un código alfanumérico aleatorio r que representa el recibo de votación. Este recibo de votación es almacenado localmente en el servidor de votación. Además, el código es cifrado con la clave g. El código alfanumérico es el recibo de votación.

6. El servidor de votación firma digitalmente el recibo de votación previamente generado y cifrado para darle validez. Entonces lo envía a la tarjeta de votación.

7. La tarjeta de votación almacena el recibo de votación cifrado después de haber verificado la firma digital del servidor de votación.

En la figura 6.3 se muestran los pasos llevados a cabo para la generación del recibo de votación.

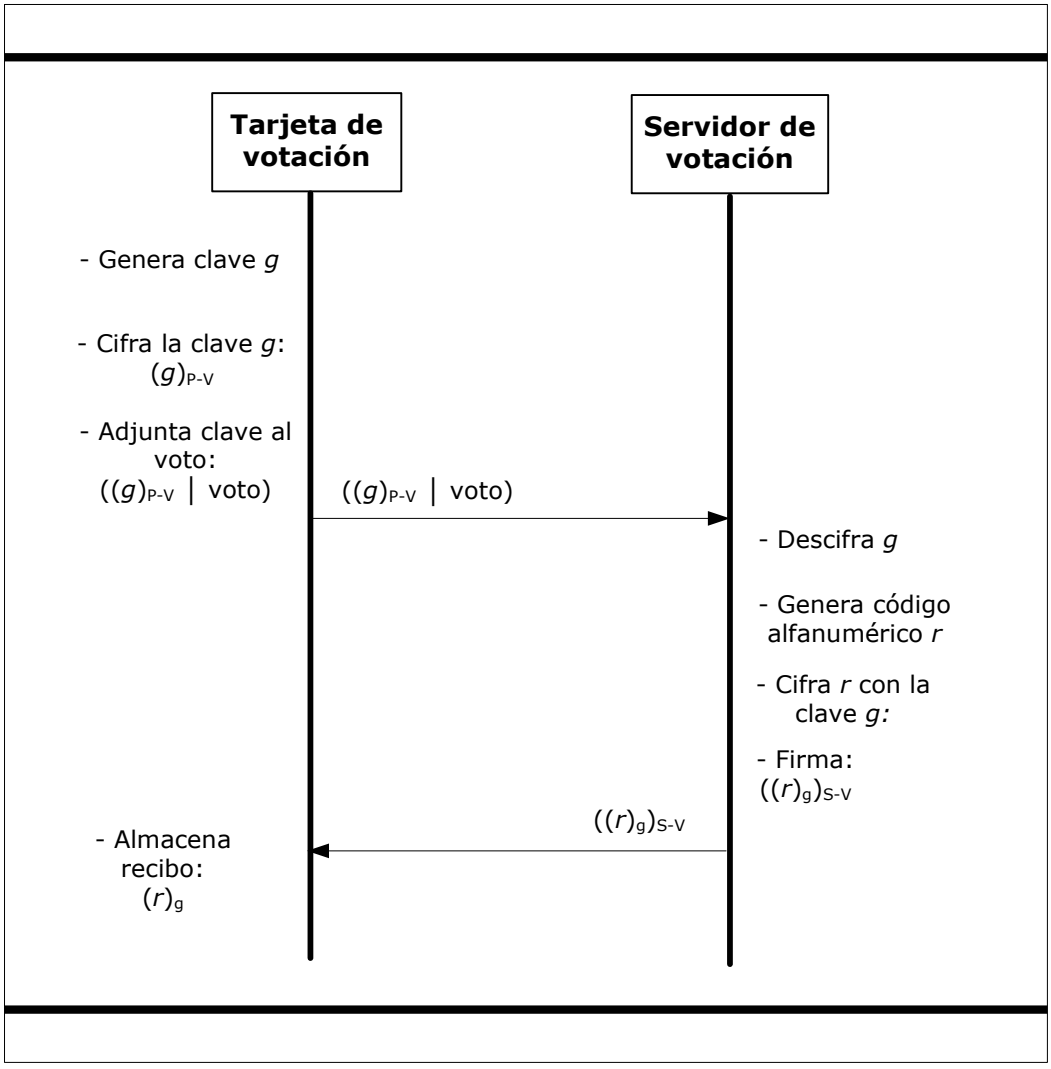

Figura 6.3. Generación del recibo de votación

Al finalizar la fase de votación se llevan a cabo las siguientes tareas:

1. Escrutinio y publicación. Los votos almacenados por el servidor de votación son validados y preparados para el escrutinio. Una vez que los votos han sido validados y contados, se publican los recibos de votación correspondientes a dichos votos.

2. Verificación. Durante el período destinado a la verificación el votante hace uso de su tarjeta de votación para acceder al sitio Web de publicación de resultados. Para tener acceso a su tarjeta, el votante debe ingresar su número de identificación personal y su huella dactilar. Habiendo sido validados ambos parámetros, la tarjeta de votación descifra el recibo almacenado utilizando la clave simétrica g. Entonces se descarga la lista publicada y se lleva a cabo una búsqueda de coincidencia entre la lista y el recibo del votante. De esta manera, el votante puede asegurarse que su voto ha sido incluido en el escrutinio. La verificación por parte de los votantes se lleva a cabo durante un período de tiempo limitado para reducir el tiempo de posibles acciones de coerción.

6.4.2 Análisis de seguridad

El recibo de votación no revela el sentido del voto, por lo que se previenen en cierta medida las prácticas de coerción. Además, estas prácticas deshonestas son reducidas gracias a que el recibo de votación es almacenado en la tarjeta de votación y por lo tanto accesible solamente por el votante legítimo.

En la sección 6.2.4 se describieron las características de seguridad que debe tener un recibo de votación. El recibo de votación propuesto cumple con dichas características tal como se muestra a continuación:

- *Resistencia a manipulaciones*. El recibo de votación es firmado digitalmente por el servidor de votación, y cuando el recibo de votación es recibido por el votante es almacenado en la tarjeta de votación. Cualquier manipulación en el recibo sería detectada al verificar la firma del servidor de votación. Por otro lado, para manipular el recibo una vez que se encuentra almacenado en la tarjeta de votación, se requeriría la colaboración del votante.

- *No repudio*. La autoridad a cargo del servidor de votación no puede negar la emisión de un recibo válido ya que este contiene la firma digital de dicho servidor. Por otro lado, el votante no puede negar la recepción de ese recibo, ya que estará almacenado en su tarjeta de votación. Esto desde luego exige ciertos requisitos a dicha tarjeta.

- *Prevención de recibos falsos*. Un votante no podría crear un recibo de votación falso ya que no posee la clave necesaria para firmarlo. Esa clave está en posesión de la autoridad a cargo del servidor de votación.

Como se ha explicado previamente, el recibo almacenado en la tarjeta de votación hace posible que los votantes verifiquen de una manera segura que su voto se ha incluido correctamente en el escrutinio. Tal como se ha descrito en la propuesta, para verificar la inclusión del voto en el escrutinio el votante debe hacer uso de su tarjeta de votación. Dicha tarjeta de votación requiere los parámetros de identidad del votante, tal como el número de identificación personal y la huella dactilar.

6.5 Propuesta de verificación: esquema basado en papeletas precifradas

A la fecha se han propuesto algunos esquemas de voto electrónico remoto que abordan el aspecto de la verificación por parte del votante, sin embargo, existen problemas para satisfacer simultáneamente ambas vertientes de la verificación individual, es decir la

verificación del registro correcto del voto y la verificación de la correcta inclusión del voto en el escrutinio.

En este esquema se tienen en cuenta algunas de las ventajas de los esquemas de papeletas precifradas y de recibos de votación ya descritos en este capítulo para cumplir con el objetivo de la verificación individual. En cuanto a las papeletas precifradas, se considera como característica esencial la propiedad de verificación que permite al votante verificar que su voto ha sido recibido correctamente por el servidor de votación. Además, en el esquema propuesto esta característica se extiende a una verificación de la correcta inclusión del voto en el escrutinio. Por lo tanto, esta propuesta combina el concepto de papeletas precifradas con un recibo de votación criptográfico a fin de tener ambas verificaciones por parte del votante.

En la fase de votación, el votante envía un código de votación que corresponde al candidato elegido. Enseguida el votante recibirá un código de verificación que corresponde al voto enviado. De esta forma, se puede llevar a cabo la primera tarea de verificación.

Durante la fase de votación, además de enviar el voto, el votante enviará información adicional que será usada para obtener un recibo de votación criptográfico firmado digitalmente por el servidor de votación. Ese recibo de votación debe contener una prueba que permite al votante verificar que su voto ha sido incluido correctamente en el escrutinio. Esto significa que el voto ha permanecido intacto desde el momento en que fue recibido por el servidor de votación hasta que se lleva a cabo el escrutinio. Por lo tanto, en este esquema el votante puede verificar ambas cosas, el registro correcto de su voto y su adecuada inclusión en el escrutinio.

Un requerimiento del esquema es que el votante debe contar con un terminal de votación con la suficiente capacidad para llevar a cabo algunas operaciones criptográficas, tal como un ordenador personal.

Las principales actividades del esquema en cada fase de la elección son las siguientes:

- Fase de preparación
    - Generación de las papeletas precifradas
    - Impresión de la información de votantes
    - Distribución de las papeletas precifradas e información de votantes

- Fase de votación
    - Generación del voto y recibo de votación
    - Envío del voto y recibo de votación
    - Validación del recibo de votación y cálculo del código de verificación
    - Verificación del votante a través del código de verificación

- Fase de consolidación de resultados
    - Descifrado de los códigos de votación
    - Escrutinio y publicación de resultados
    - Verificación del votante a través del recibo de votación

Estas actividades serán detalladas a continuación. La tabla 6.1 describe la nomenclatura usada en el protocolo.

6.5.1 Fase de preparación

Generación de las papeletas precifradas

A diferencia de los esquemas convencionales de voto electrónico, en los cuáles las operaciones criptográficas son principalmente aplicadas durante la fase de votación, en un esquema de papeletas precifradas las principales operaciones de cifrado son llevadas a cabo durante la generación de las papeletas precifradas, es decir, en la fase de preparación.

Tabla 6.1. Nomenclatura

Símbolo	Descripción
Cod	Código de votación
Ver	Código de verificación
P-Id	Identificador de papeleta
C-Id	Identificador de candidato
R-Id	Identificador de recibo de votación
E-Id	Identificador de la elección
VS	Servidor de votación
CS	Servidor de escrutinio
P-VS	Clave pública del servidor de votación
P-CS	Clave pública del servidor de escrutinio
r	Datos del recibo de votación
R	Recibo de votación
S	Secreto generado por el votante
V	Mensaje de voto generado por el votante
Sv	Clave privada del votante
S-VS	Clave privada del servidor de votación
S-CS	Clave privada del servidor de escrutinio
Sk	Clave simétrica aleatoria
Inter	Valor intermedio para generar códigos de votación
A	Valor aleatorio para generar códigos de votación
B	Valor aleatorio para generar códigos de verificación
KA	Sobre digital pata proteger *A*
KB	Sobre digital pata proteger *B*
$\oplus$	Operación XOR entre dos valores
$(x \mid y)$	Concatenación de “x” con “y”

La generación de las papeletas precifradas constituye un aspecto muy importante en la seguridad del esquema de votación. Por lo tanto, es necesario definir algunas medidas y procedimientos que garanticen un ambiente seguro para su generación. Por ejemplo, es importante llevar a cabo el proceso de generación en un ambiente aislado a fin de prevenir intrusiones que podrían alterar el proceso o incluso obtener información generada en dicho proceso.

Los códigos de votación deben ser códigos únicos y su longitud debe cumplir un compromiso entre seguridad y usabilidad. Por otro lado, los códigos de verificación pueden ser códigos únicos pero su longitud es más flexible ya que el votante no tiene que introducirlo sino sólo verificarlo.

Sea *m* el número de candidatos que participarán en la elección, y *n* el número de votantes potenciales, se requiere:

- *m* identificadores de votantes,
- *n* x *m* códigos de votación, y
- *n* x *m* códigos de verificación

Los códigos de votación y verificación son generados de la siguiente forma:

1. Generación de identificadores únicos de papeletas ($P\text{-}Id_i$). Esta generación se lleva a cabo de manera aleatoria. El identificador de la papeleta es un valor numérico que será convertido a su representación binaria a fin de ser operado con otros valores.

2. Generación de identificadores únicos de candidatos ($C\text{-}Id_j$). Un valor numérico que representa el identificador del candidato es asignado a cada candidato. Al igual que en el caso de los identificadores de las papeletas, los identificadores de candidatos son convertidos a su representación binaria.

3. Para cada identificador de papeleta $P\text{-}Id_i$:
    - Se generan dos valores binarios aleatorios A_i y B_i.
    - Para cada identificador de candidato $C\text{-}Id_j$:
        - $P\text{-}Id_i$ y $C\text{-}Id_j$ son operados con un XOR, obteniendo un valor intermedio *Inter*:

$$Inter_{i,j} = (P\text{-}Id_i \oplus C\text{-}Id_j)$$

- $Inter_{i,j}$ y A_i son operados con un XOR. El resultado es el código de votación $Cod_{i,j}$:

$$Cod_{i,j} = (Inter_{i,j} \oplus A_i)$$

- Se genera una clave simétrica aleatoria $k1_i$.
- El valor A es cifrado con la clave $k1_i$.
- La clave $k1_i$ es cifrada con la clave pública *P-CS,* la cuál pertenece a la autoridad de la elección a cargo del escrutinio. El resultado de ambas operaciones de cifrado es un sobre digital de la forma:

$$KA_i = ((A)_{k1i}\ ,\ (k1_i)_{P\text{-}CS})$$

- Un código de verificación $Ver_{i,j}$ correspondiente a cada código de votación $Cod_{i,j}$ es entonces generado:
  - $P\text{-}Id_i$ y $Cod_{i,j}$ (su representación binaria) son operados con un XOR.
  - B_i y el valor previamente obtenido también son operados con un XOR. El resultado de estas operaciones es el código de verificación:

$$Ver_{i,j} = (B_i \oplus (P\text{-}Id_i \oplus Cod_{i,j}))$$

- Se genera una clave simétrica aleatoria $k2_i$.
- El valor B_i es entonces cifrado con la clave $k2_i$ y esta clave a su vez es cifrada con la clave pública *P-VS,* la cuál pertenece al servidor de votación:

$$KB_i = ((B)_{k2i}\ ,\ (k2_i)_{P\text{-}VS})$$

4. El valor KA_i y su correspondiente $P\text{-}Id_i$ son transferidos a la autoridad de escrutinio:

$$\{(P\text{-}Id_1,\ KA_1),\ (P\text{-}Id_2\ ,\ KA_2)\ \ldots\ (P\text{-}Id_n\ ,\ KA_n)\}$$

   Esta transferencia se lleva a cabo al finalizar el proceso de generación de papeletas. El valor A será usado por la autoridad de escrutinio durante el descifrado de los códigos de votación, tal como será descrito más adelante.

5. El valor KB_i junto con su correspondiente $P\text{-}Id_i$ son almacenados en el servidor de votación:

$$\{(P\text{-}Id_1\,,\, KB_1), (P\text{-}Id_2\,,\, KB_2)\ \ldots\ (P\text{-}Id_n\,,\, KB_n)\}$$

   El valor B será descifrado y utilizado por el servidor de votación cuando el voto se recibe, para calcular el código de verificación, tal como será explicado más adelante.

La figura 6.4 muestra el proceso de generación de códigos descrito previamente. Algunos de los valores generados durante el proceso de generación de las papeletas precifradas podrían ser usados de manera maliciosa para violar la privacidad de los votantes. Por lo tanto, es importante que al terminar el proceso, dichos valores sean eliminados de una manera segura. Estos valores incluyen: $Inter_{i,j}$, A_i, y B_i.

A fin de que la clave privada (*S-CS*) que se usará para descifrar los códigos de votación se mantenga protegida será partida en segmentos. Aprovechando el hecho de que la mesa electoral encargada del escrutinio es usualmente conformada por personas de diferentes partidos o intereses, cada miembro de dicha mesa electoral poseerá un segmento de la clave privada. De esta forma, el descifrado de los códigos de votación puede llevarse a cabo solamente con la cooperación del total o de un subconjunto predefinido de los miembros de la mesa electoral, tal como se describe en [IS90] y en [Pe91]. La segmentación de la clave privada se puede llevar a cabo utilizando un esquema de secreto compartido como el descrito por Shamir [Sh79].

Los códigos de verificación no son impresos en las papeletas precifradas a fin de prevenir el acceso y control de los códigos de votación y verificación por parte de un atacante. En lugar de imprimirlos, los códigos de verificación se hacen accesibles a los votantes a través de un sitio Web. De esta forma se previenen los ataques que traten de manipular en la papeleta la relación de los pares de códigos con los candidatos para cambiar la

intención del votante. A fin de acceder al sitio Web, el votante requerirá de una contraseña que es generada y asociada al identificador de la papeleta.

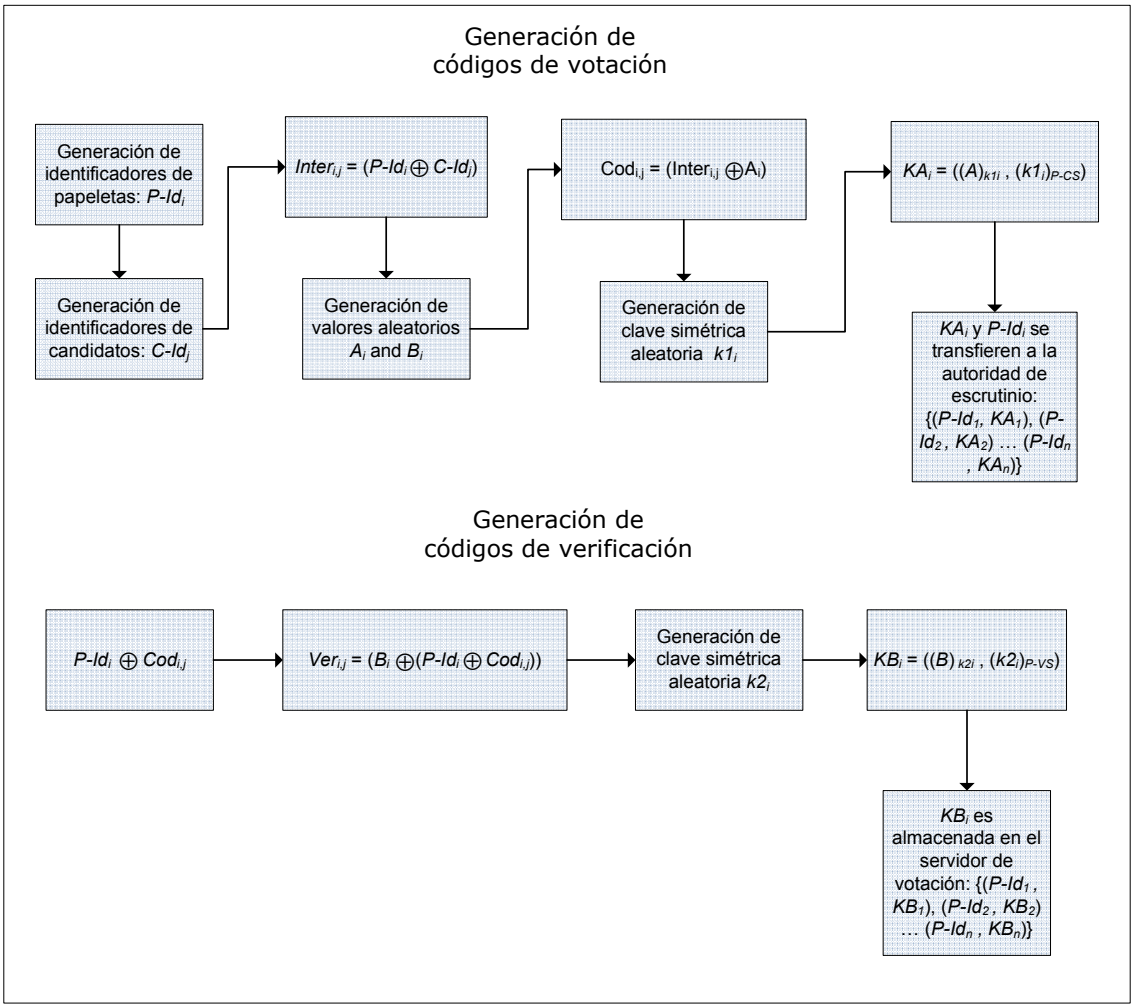

Figura 6.4 Proceso de generación de códigos de votación y verificación

Una vez que los elementos necesarios han sido generados, las papeletas precifradas son creadas al imprimir los siguientes elementos:

- El identificador de la papeleta $P\text{-}Id_i$.
- Nombres de candidatos, partidos, afiliación, etc.
- Códigos de votación.

- Contraseña para obtener los códigos de verificación (con cubierta de protección de látex).

Los pares compuestos por nombre de candidato y código de votación son impresos en un orden aleatorio. Esta aleatoriedad evitará algunos ataques de privacidad y coerción. La figura 6.5 muestra un ejemplo de papeleta precifrada utilizada en el esquema.

Impresión de la información de votantes

En adición a las papeletas precifradas, se imprime otra hoja con la información de votante:

- Nombre
- Dirección
- Información adicional (del votante o de la elección)
- Información para obtener los códigos de verificación (sitio Web, instrucciones, etc.)

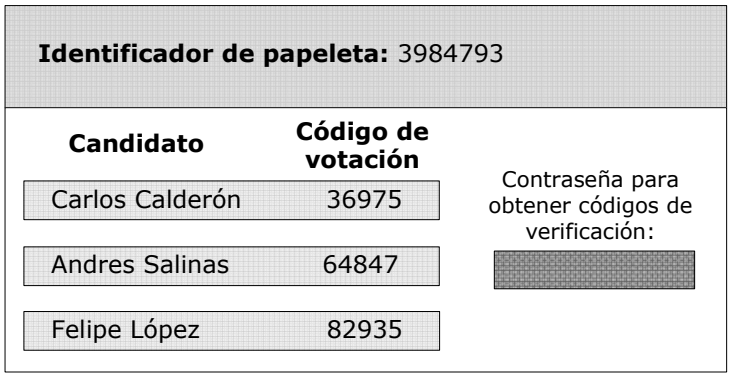

Figura 6.5. Ejemplo de papeleta precifrada usada en el esquema

Distribución de las papeletas precifradas e información de votantes

La asignación de las papeletas precifradas es anónima por medio de un proceso de asignación aleatorio. Se forman paquetes que contienen una papeleta precifrada y una hoja de información de votante sin relación entre ellas. Se requieren procedimientos de

seguridad que permitan esta asignación de manera anónima. Por ejemplo, una vez que las hojas de información de votantes son impresas, cada una de ellas es sellada y entonces asignada a un paquete.

La entrega de los paquetes a los votantes se lleva a cabo a través de un canal de comunicación presumiblemente seguro, por ejemplo servicio postal u otro servicio de distribución de mensajería.

Es importante notar que además de las medidas de seguridad previamente descritas para la generación y distribución de las papeletas precifradas e información de votantes, se pueden emplear medidas de seguridad adicionales tal como el uso de papel que contenga elementos de seguridad para detectar manipulaciones o falsificaciones.

Una vez que el votante ha recibido su papeleta precifrada y su hoja de información de votante, puede obtener los códigos de verificación accediendo al sitio Web especificado. En dicho sitio Web, el votante debe especificar el identificador de su papeleta y la contraseña asociada. Entonces, los códigos de verificación se le muestran en el mismo orden en que se encuentran impresos los códigos de votación en su papeleta, de tal forma que el votante pueda relacionarlos sin dificultad. El uso de la contraseña previene que algún atacante obtenga códigos de verificación del sitio Web simplemente al tratar con identificadores de papeleta aleatorios.

6.5.2 Fase de votación

En este punto del proceso el votante ya cuenta con su papeleta precifrada y los correspondientes códigos de verificación. El canal de comunicación entre el terminal de votación y el servidor de votación es protegido usando el protocolo TLS. Se asume que los votantes cuentan con un certificado digital para autenticarse a fin acceder a la plataforma de votación. A continuación se muestran los pasos para emitir los votos y generar los recibos de votación.

Generación del voto y del recibo de votación

1. El votante escoge su voto a través del correspondiente código de votación ($Cod_{i,j}$).

2. Se genera aleatoriamente un identificador único $R\text{-}Id_i$.

3. El identificador único y el identificador de la elección se concatenan y se calcula un hash de dicha concatenación. Este valor es firmado digitalmente por el votante. Esta información es utilizada para generar un recibo de votación r_i:

$$r_i = (\mathrm{H} [R\text{-}Id_i \mid E\text{-}Id])_{Sv}$$

4. El votante genera un secreto S que consiste en calcular un hash del código de votación y concatenarlo con el identificador único. Este secreto será utilizado para verificar si el voto es incluido en el escrutinio. El secreto es cifrado con la clave pública de la autoridad de escrutinio:

$$S_i = ((\mathrm{H} [Cod_{i,j}] \mid R\text{-}Id_i)_{Sv})_{P\text{-}CS}$$

Envío del voto y recibo de votación

El votante envía el mensaje de voto V al servidor de votación. El mensaje V se compone del código de votación, la información del recibo de votación, el secreto y el identificador de la papeleta:

$$V_i: Cod_{i,j} \mid r_i \mid S_i \mid P\text{-}Id_i$$

Validación del recibo de votación y cálculo del código de verificación

Cuando el servidor de votación recibe el mensaje V_i, lleva a cabo las siguientes tareas:

1. Verificación de la legitimidad del votante a través de la firma digital en r_i

2. Validación del recibo de votación R_i firmando digitalmente r_i:

$$R_i = (r_i)_{S\text{-}VS}$$

3. Cálculo del código de verificación $Ver_{i,j}$ que corresponde al código de votación $Cod_{i,j}$:
   - El servidor de votación descifra el valor B_i que corresponde al $P\text{-}Id_i$ recibido.
   - Entonces, el servidor de votación calcula:

$$Ver_{i,j} = (B_i \oplus (P\text{-}Id_i \oplus Cod_{i,j}))$$

4. El recibo de votación R_i y el código de verificación $Ver_{i,j}$ son enviados al votante.

5. El código de votación $Cod_{i,j}$ es cifrado con la clave pública del servidor de escrutinio a fin de mantenerlo protegido durante la fase de votación:

$$Cod'_{i.j} = (Cod_{i.j})_{P\text{-}CS}$$

6. Los valores $Cod'_{i,j}$, S_i, y $P\text{-}Id_i$ son firmados digitalmente por el servidor de votación y almacenados junto con R_i:

$$(Cod'_{i.j} , S_i, P\text{-}Id_i)_{\text{S-VS}}$$

<u>Verificación del votante a través del código de verificación</u>

El votante recibe el código de verificación $Ver_{i,j}$ y verifica que tal código corresponde al código de votación emitido por Él (verificación del registro correcto). Si la verificación es correcta, el votante almacena o imprime el recibo de votación R_i y su sesión de voto es finalizada.

La figura 6.6 muestra los pasos llevados a cabo por el terminal y el servidor de votación durante el proceso de votación.

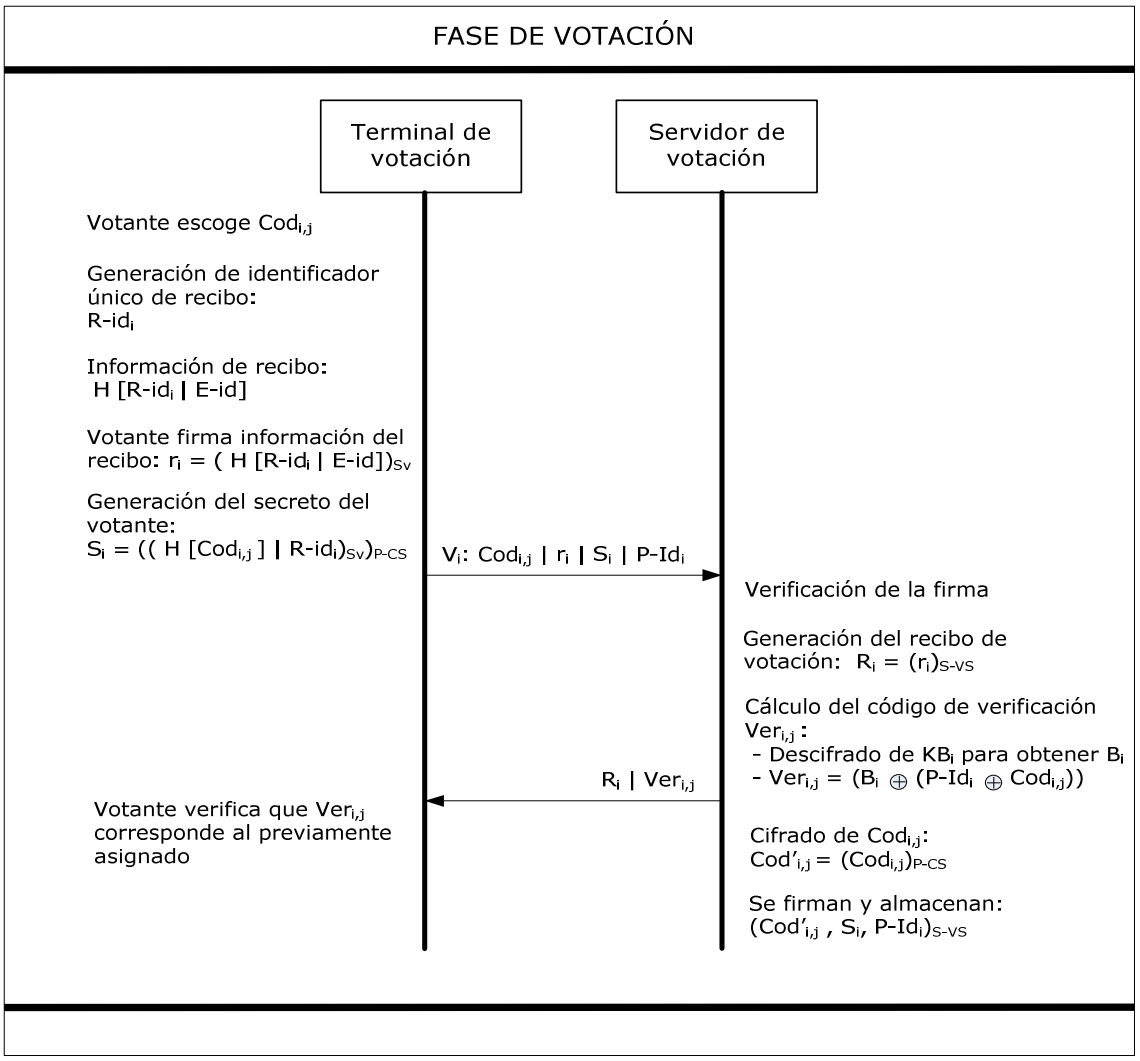

Figura 6.6. Generación e intercambio de mensajes en el proceso de votación

6.5.3 Fase de consolidación de resultados

Una vez que la fase de votación ha finalizado se puede llevar a cabo la consolidación de resultados.

Descifrado de los códigos de votación

Para llevar a cabo el descifrado de los códigos de votación se siguen los siguientes pasos, tal como se muestra en la figura 6.7:

1. Los miembros de la autoridad de escrutinio (mesa electoral) descargan el conjunto de códigos de votación y secretos de los votantes que están almacenados en el servidor de votación.

2. Los códigos de votación $Cod'_{i,j}$ que fueron cifrados en el servidor de votación, son ahora descifrados con la clave privada de la autoridad de escrutinio.

3. Los secretos S_i son descifrados para obtener los valores hash de los códigos de votación.

4. Se calcula el valor hash de cada código de votación para compararlo con el valor hash obtenido del secreto. De esta forma es posible verificar si el código de votación se ha mantenido inalterable desde el momento en que fue enviado por el votante.

5. El valor $R\text{-}Id_i$ obtenido del secreto es comparado con el $R\text{-}Id_i$ incluido en r_i.

6. Los códigos de votación son descifrados para obtener el candidato que corresponde. El descifrado del código de votación se lleva a cabo de la siguiente manera:
    - Los códigos de votación $Cod_{i,j}$ son convertidos a su representación binaria.
    - El valor A_i es descifrado usando la clave privada de la autoridad de escrutinio. En realidad, esta clave permite el descifrado de la clave privada necesaria para descifrar A_i.
    - Se calcula el XOR de $Cod_{i,j}$ y su correspondiente A_i para obtener el valor $Inter_{i,j}$.
    - Se calcula el XOR de $Inter_{i,j}$ y su correspondiente $P\text{-}Id_i$ para obtener el identificador del candidato $C\text{-}Id_j$.

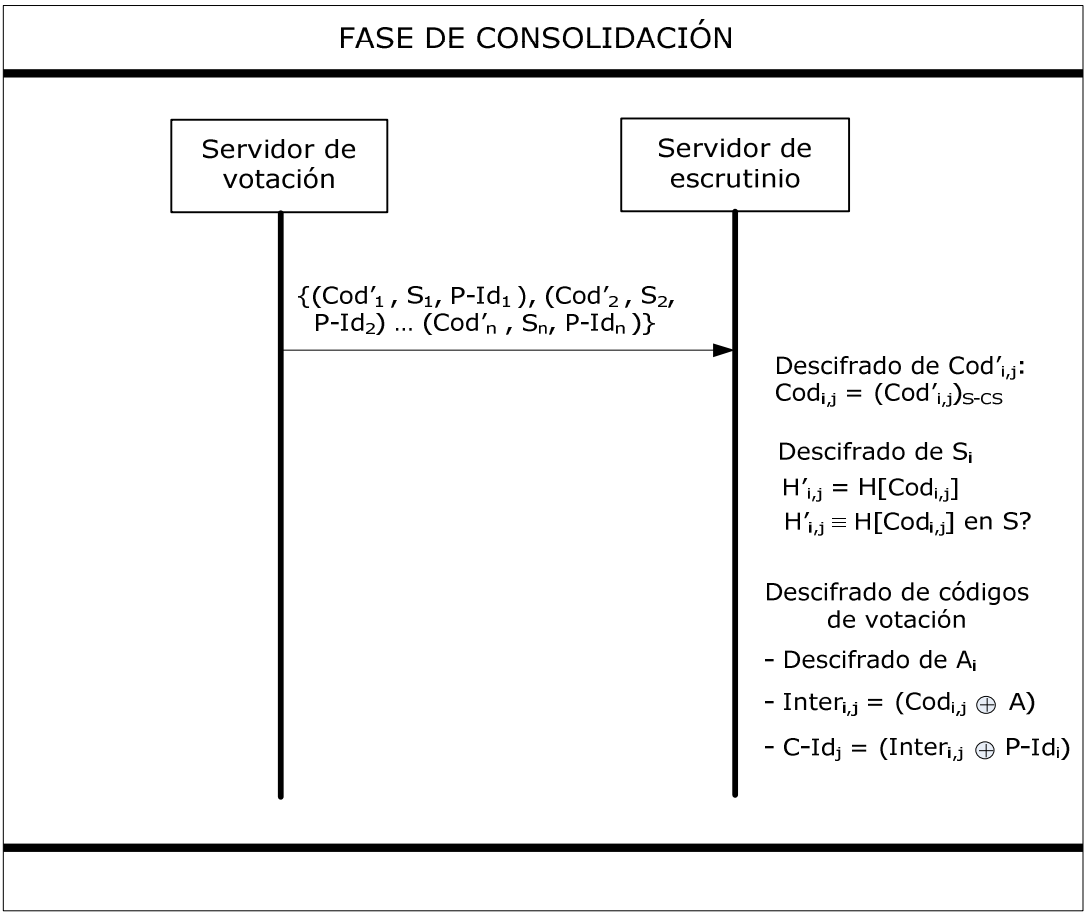

Figura 6.7. Descifrado de códigos en la fase de consolidación

Escrutinio y publicación de resultados

Los identificadores de candidato obtenidos en el paso previo son asociados a los nombres de los candidatos. Entonces, se lleva a cabo el escrutinio de los votos. Los resultados de la elección y la lista de los *R-Id's* obtenidos de los secretos generados por los votantes son publicados a través de un sitio Web.

Verificación del votante a través del recibo de votación

El votante accede al sitio web de publicación de resultados y verifica que su $R\text{-}Id_i$ se encuentra incluido en la lista de *R-Id*'s. Con esta verificación el votante comprueba que su voto ha permanecido inalterable desde su envío y que ha sido incluido correctamente en el escrutinio (verificación de escrutinio correcto). En el caso de que su $R\text{-}Id_{i,}$ no esté en

la lista publicada, el votante puede reclamar a la autoridad de la elección mostrando su recibo de votación R_i.

6.5.4 Análisis de seguridad

Se describen a continuación los principales ataques que amenazan la seguridad de los esquemas de voto por Internet en general y de papeletas precifradas en particular y se analiza como estos ataques son mitigados o al menos disminuidos con el esquema propuesto:

- *Software malicioso.* Uno de los principales problemas del voto por Internet es el riesgo de inserción de software malicioso en el terminal de votación, el cuál es usualmente un ordenador personal. Este ataque podría desvelar o cambiar la intención de voto del votante sin la posibilidad de detección. En el esquema propuesto, tal como en la mayoría de los esquemas de papeletas precifradas, si un código de votación es capturado por ejemplo a causa de software malicioso, el atacante no puede saber a favor de cuál candidato es ese voto. Por otro lado, si el código de votación es modificado por un atacante, existe una probabilidad mínima de que el nuevo código de votación sea uno válido. Además si la modificación del código de votación resultara en otro código de votación válido, esto sería detectado por el votante al recibir un código de verificación que no corresponde. Por lo tanto, si un atacante intenta manipular el voto a través de software malicioso para obtener una ventaja para un candidato específico, debería primeramente conocer el código de votación que corresponde a ese candidato, y debido a que el código de votación es único, el ataque es improbable.

- *Manipulación de las papeletas precifradas.* Un intento de modificar una papeleta precifrada, con el propósito de que el votante envíe un voto diferente a su intención sin que pueda darse cuenta de ello, es evitado al separar los pares de códigos. Tal como se ha descrito previamente, en esta propuesta los códigos de votación son impresos en la papeleta y los códigos de verificación son solo

accesibles a través de un sitio Web que requiere una contraseña. De esta forma, un atacante que intercepte la papeleta precifrada, por ejemplo durante su transporte, puede cambiar sólo el orden de los códigos de votación sin embargo este tipo de manipulación será detectada una vez que el votante envíe el código de votación y reciba como respuesta un código de verificación que no corresponde al candidato elegido.

- *Privacidad.* Las condiciones para llevar a cabo un ataque exitoso que logre violar la privacidad del votante en un esquema de papeletas precifradas han sido descritas previamente en la sección 6.3.1. En el esquema propuesto, la asignación aleatoria y anónima de las papeletas precifradas disminuye considerablemente la posibilidad de violación de la privacidad. Además, el esquema está preparado para prevenir ataques que intenten desvelar la opción elegida por el votante. Tal como se ha expuesto en la descripción de la propuesta, cuando un código de votación es recibido por el servidor de votación, dicho código se cifra con la clave pública de la autoridad de escrutinio. Este cifrado es principalmente propuesto debido al hecho de que durante la fase de votación el servidor de votación está en línea y por lo tanto expuesto a ataques remotos.

- *Coerción.* Una vez que la privacidad de los votantes es protegida a través de los medios y técnicas ya descritas, las prácticas de coerción o venta de votos son considerablemente disminuidas. Además, los códigos de votación enviados por los votantes no son publicados a fin de prevenir otras posibilidades de coerción. El ataque clásico de coerción de los sistemas de voto remoto continua sin resolverse. En este ataque, el votante debe votar en presencia del atacante para que este pueda estar seguro de que el votante ha cumplido con la coacción. Sin embargo, la posibilidad de llevar a cabo un ataque de coerción a gran escala es eliminada empleando las técnicas descritas en esta propuesta.

Se ha llevado a cabo una comparación del esquema propuesto con otros esquemas de votación que consideran la verificación individual como parte fundamental. Esta

comparación se presenta en la tabla 6.2. Uno de los esquemas utilizados para la comparación es la propuesta más significativa a la fecha basada en boletas precifradas [SD05]. El segundo esquema utilizado en esta comparación incluye un recibo criptográfico de votación [Sa94], sin embargo dicho esquema presenta las mismas características evaluadas que la mayoría de los esquemas con recibos de votación.

El esquema propuesto cumple con los dos objetivos de la verificación individual, es decir, la verificación del registro correcto y la verificación de escrutinio correcto. Por medio del código de verificación el votante puede estar seguro que su voto fue recibido correctamente en el servidor de votación. Además, el recibo criptográfico que incluye el esquema permite al votante verificar que su voto es incluido en el escrutinio. De esta forma, el esquema que se ha presentado considera el ciclo completo de verificación individual, desde la recepción del voto en el servidor de votación hasta la inclusión de dicho voto en el proceso de escrutinio.

Tabla 6. 2. Comparativa de esquemas de verificación

Factor de comparación	**Esquema basado en papeletas precifradas [SD05]**	**Esquema que incluye un recibo criptográfico de votación [Sa94]**	**Esquema propuesto**
Verificación de registro correcto	Sí	No	Sí
Verificación de escrutinio correcto	Parcial	Sí (condicionado a registro correcto)	Sí
Prevención de software malicioso	Sí	No	Sí
Prevención de manipulación de papeleta	Parcial	N/A	Sí
Protección de privacidad	Parcial	Sí	Sí
Prevención de coerción	Parcial	Parcial	Parcial

En este esquema de votación por Internet, un ataque de inserción de software malicioso en el terminal de votación no es suficiente para llevar a cabo un ataque exitoso que trate de manipular el voto o descubrir la opción de voto elegida por el votante. Además, se ha descrito como se previene un ataque de manipulación de la papeleta al separar los códigos de votación y verificación. Los códigos de votación son impresos en la papeleta, sin embargo, los códigos de verificación son solamente accedidos por el votante a través de un sitio Web que requiere el identificador de la papeleta y una contraseña asociada a dicho identificador.

Por otro lado, a fin de proteger la privacidad se han considerado diferentes aspectos. La distribución de las papeletas precifradas a los votantes se lleva a cabo por medio de un proceso de asignación aleatoria que previene que autoridades maliciosas de la elección mantengan una relación de códigos con votantes. De manera adicional, los códigos de votación se cifran una vez que han sido recibidos por el servidor de votación. De esta forma se logra la protección de dichos códigos durante su almacenamiento en el servidor de votación, es decir, durante todo el período de votación.

Debido a que un sistema de votación basado en papeletas precifradas no es la forma de votación convencional, un esquema como el propuesto no es la mejor opción en cuanto a usabilidad se refiere. Por esta razón se aconseja: i) introducirlo como un canal de votación alternativo y de manera simultánea con sistemas de votación convencionales, y ii) implementarlo en elecciones con una cantidad baja de asuntos sometidos a votación.

6.6 Conclusiones y aportación

En este capítulo se han descrito los diferentes mecanismos que permiten al votante verificar la integridad de su voto. Se han analizado los sistemas de verificación independiente propuestos en [VVSG06] y se ha concluido que, con la excepción de los sistemas de verificación con cifrado extremo a extremo, no es posible implementarlos de manera eficiente en el voto electrónico remoto. También se han analizado las propiedades

de verificación de un tablón de anuncios electrónico y de los esquemas de papeletas precifradas, los cuáles son apropiados para implementaciones de voto electrónico en entornos remotos.

Se han presentado además en este capítulo dos aportaciones enfocadas a la verificación individual. La primera de ellas (sección 6.4) consiste en un recibo de votación criptográfico que puede sea adaptado a diferentes esquemas remotos de votación. La definición y características de dicho recibo criptográfico han sido publicadas en [MSM+08]. El recibo de votación cumple con las características esenciales de seguridad que le permiten al votante verificar la inclusión de su voto en el escrutinio.

La segunda aportación presentada en este capítulo (sección 6.5) consiste en un esquema de verificación basado en papeletas precifradas. El esquema propuesto cumple con los dos aspectos de verificación individual (registro y escrutinio correcto), que considero necesarios para que un sistema de votación sea fiable. Este esquema de votación ha sido presentado para su revisión en la revista “Computer Communications”.

Capítulo 7

Consolidación de Resultados de Votación

7.1 Introducción

En un proceso de elección, la precisión en los resultados es un requerimiento esencial. Tradicionalmente, el escrutinio de los votos se ha llevado a cabo manualmente, lo que tiene como consecuencia un retraso no deseado en la publicación de resultados y sobretodo una alta probabilidad de cometer errores.

La modernización de los sistemas de votación ha permitido agilizar el escrutinio de los votos y la precisión en los resultados mediante el uso de dispositivos electrónicos (p.e., terminales de voto electrónico o máquinas de escaneo de votos). Estos dispositivos permiten generar un registro electrónico de los votos, y por lo tanto se puede llevar a cabo un proceso de escrutinio electrónico de una manera más rápida y fiable.

A pesar de dicha modernización, la integridad en un proceso de consolidación de resultados puede verse afectada por prácticas fraudulentas o por simples descuidos del personal que participa en dicho proceso. Por esta razón, es necesario definir mecanismos que ayuden a proteger la integridad de los resultados.

7.2 Proceso de consolidación de resultados

En un sistema de voto electrónico remoto el proceso de escrutinio es simple, ya que usualmente los votos se reciben en un servidor central. Por lo tanto, una vez que la fase de votación ha concluido se procede a llevar a cabo el descifrado (si fuera el caso) y el escrutinio de los votos. Sin embargo, en elecciones en las que se utilizan distintos canales de votación de manera simultánea se presenta un problema para llevar a cabo el escrutinio de los votos. Esto se debe a que primeramente es necesario realizar un proceso de consolidación de votos para después llevar a cabo el escrutinio. Por ejemplo, para una elección presidencial se podrían utilizar una variedad de canales de votación: voto electrónico a través de terminales DRE, votación con terminales de reconocimiento óptico de marcas, voto postal, voto electrónico remoto para residentes en el extranjero (voto por fax, correo electrónico e Internet), etc. Esta variedad de canales tiene como consecuencia que a la hora de consolidar los resultados a partir de los distintos canales de votación se presenten serias complicaciones que podrían llegar a alterar los resultados reales.

El proceso de escrutinio en el ejemplo descrito anteriormente se lleva a cabo de manera independiente en cada canal de votación (por ejemplo en el voto postal) y en cada unidad electoral (por ejemplo un recinto electoral en donde se utilizan terminales DRE) y posteriormente se lleva a cabo una consolidación global de todos los resultados obtenidos en cada uno de los canales de votación u unidad electoral. La complejidad del proceso se incrementa si consideramos necesario obtener previamente los resultados por municipio, por provincia, etc., y posteriormente llevar a cabo una consolidación global. En la figura 7.1 se muestra un ejemplo de esquema de consolidación de resultados en un entorno de elección con múltiples canales de votación.

El proceso de escrutinio de los votos en una elección cuenta con diferentes niveles de consolidación. Cada nivel es una entidad que necesita llevar a cabo el escrutinio de los votos pertenecientes a las entidades de un nivel inferior de consolidación. Por ejemplo, una provincia necesitará consolidar los resultados de los municipios que le pertenecen.

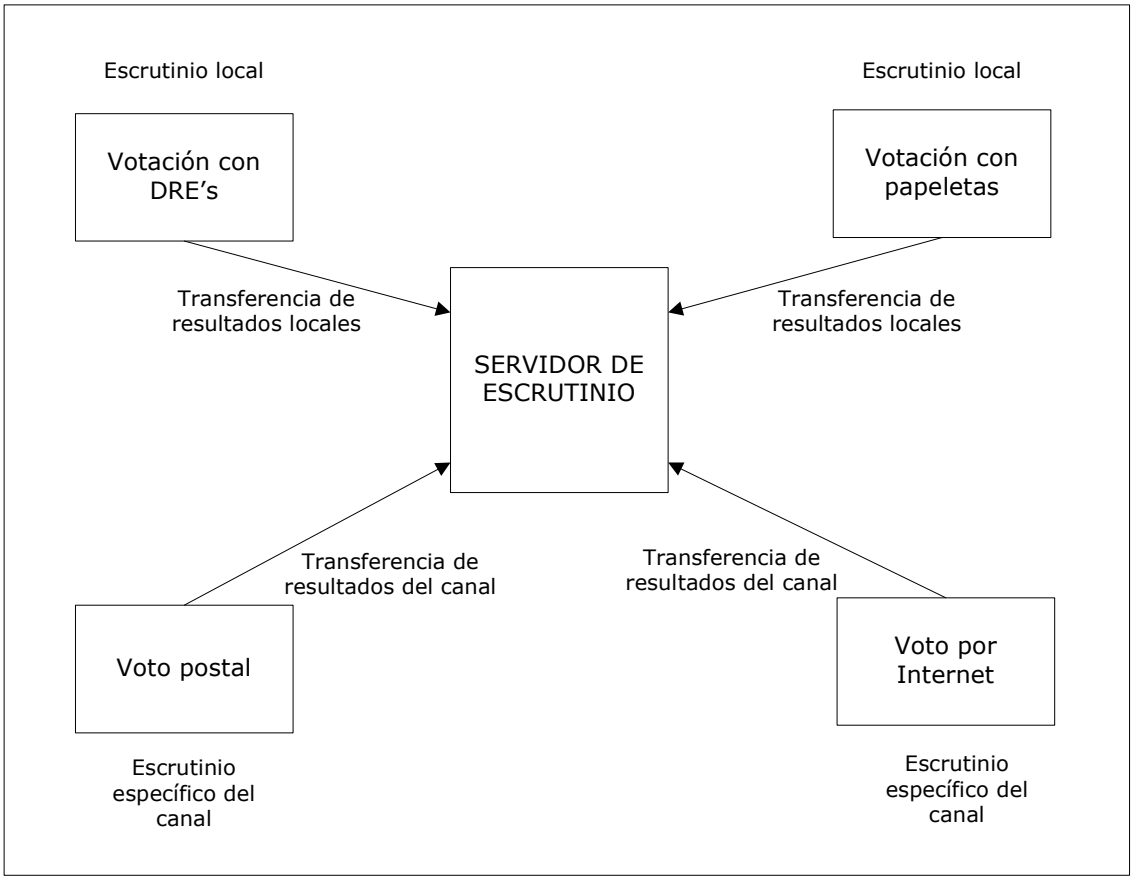

Figura 7.1. Esquema de consolidación en una elección con múltiples canales de votación

Por lo tanto, un proceso de consolidación de resultados generalmente lleva a cabo los siguientes pasos:

1. Consolidación. Cada nivel de consolidación recibe los resultados de las entidades de nivel inferior.
2. Escrutinio. Cada nivel de consolidación lleva a cabo el escrutinio (o la suma) de los resultados intermedios recibidos.
3. Transferencia y/o publicación. Cada nivel de consolidación transfiere a un nivel de consolidación superior los resultados obtenidos en el escrutinio. Si es el caso, publica dichos resultados.

Por otro lado, para que un sistema de consolidación de resultados sea eficiente y seguro, debe satisfacer los siguientes requerimientos:

- *Protección de la privacidad*. Los votos deben mantenerse protegidos durante el proceso de consolidación. Usualmente esto se logra por medio del cifrado de los votos en el terminal de votación.

- *Facilidad de auditoria de resultados intermedios*. En un proceso de consolidación de resultados se deben proveer medidas que faciliten auditar la integridad de los resultados locales e identificar si estos resultados han sido avalados por las autoridades encargadas de realizar el escrutinio correspondiente. Es decir, debe ser posible verificar de una forma fehaciente si los escrutinios locales recibidos por el centro de consolidación han sido manipulados.

- *Integridad de los resultados globales*. Además de las medidas que se deben tomar en cuenta para verificar la integridad de los resultados intermedios también se debe considerar la protección de la integridad en el último paso del proceso de consolidación, es decir en el escrutinio final de resultados globales.

- *Flexibilidad*. Un sistema de consolidación debe tener en cuenta la posibilidad de consolidar resultados que provengan de distintos canales de votación.

En los sistemas de consolidación de resultados propuestos a la fecha, por ejemplo [Sc03 y KK06], no se considera la protección de los resultados intermedios, es decir, no se han planteado técnicas que garanticen la integridad de los resultados intermedios antes de ser enviados ni tampoco que puedan garantizar la integridad del resultado final.

Debido a la posibilidad de manipulación de los resultados, existen métodos que pretenden verificar (o auditar) la precisión en el resultado de una elección mediante registros paralelos en diferentes soportes de almacenamiento. Un ejemplo de esto son los sistemas

de verificación independiente definidos en [VVSG06] y descritos previamente en el capítulo 6. El problema principal de estos sistemas es que si uno de los dos registros es manipulado durante la fase de votación, es difícil saber cuál de ellos ha sido y por lo tanto no se tiene la certeza de cuál resultado es el correcto.

7.3 Esquema seguro y auditable de consolidación de resultados

La propuesta que se presenta a continuación describe un esquema de consolidación de resultados de un proceso electoral. El principal objetivo del esquema propuesto es proteger la integridad de los resultados intermedios de la elección, así como comprobar la autoría del oficial o de los oficiales de la elección que generan y envían dichos resultados. Además, el esquema permite generar registros físicos de los resultados intermedios y proteger su integridad.

Como parte del esquema también se describen los procesos que permiten validar de forma robusta la identidad de oficiales de la elección que han participado en la validación de los resultados generados en sus respectivas unidades electorales. Eso se hace con el fin de verificar si los resultados electorales locales validados son los mismos que se van a consolidar.

El esquema propuesto puede ser utilizado en la consolidación de resultados en un entorno remoto de votación. Sin embargo, además se tiene en cuenta que en un proceso de elección puede haber diferentes canales de votación, entre los que se incluyen sistemas de voto presencial y remotos, por lo que el esquema se aplica también a elecciones que contemplan esta posibilidad.

Participantes del esquema

Para el esquema propuesto se considera la participación y colaboración de las siguientes entidades:

Unidad electoral. En el esquema definiremos una unidad electoral como cualquier entidad en donde se generen resultados intermedios de la elección. Esto puede ser un recinto electoral, un distrito, etc. Un canal de voto electrónico remoto también será considerado como una unidad electoral.

Módulo de consolidación. En el módulo de consolidación se lleva a cabo la recepción de los resultados generados en un nivel inferior de consolidación. El módulo de consolidación generalmente es parte de una unidad electoral que recibe resultados de unidades electorales de nivel inferior. Este módulo verifica que dichos resultados intermedios hayan sido validados por las autoridades electorales locales correspondientes, y comunica el resultado de esa verificación a dichas autoridades. Para facilitar la comunicación remota entre el módulo de validación y las autoridades electorales locales se requiere de una conexión remota que puede ser a través de Internet.

Oficial de la elección. Cada uno de los oficiales que forman parte de la gestión de una unidad electoral. La función principal de los oficiales de la elección es la validación de los resultados de su unidad electoral. Los oficiales de la elección también participan en la obtención del escrutinio local y en la comunicación de los resultados al nivel de consolidación superior. También se encargan de generar un acta oficial en papel de los resultados locales de su unidad electoral.

Para fines del esquema propuesto, es importante señalar que en la validación de resultados de una unidad electoral pueden participar representantes de partidos políticos, por lo que dicha responsabilidad no recae solamente en la autoridad de la elección.

7.3.1 Fases del proceso de consolidación

Una vez que se ha hecho el escrutinio de los votos en una unidad electoral se obtiene la información de los resultados intermedios. Entonces se lleva a cabo el proceso de consolidación de resultados en las siguientes fases:

- Generación y transferencia de la prueba de validación.
- Verificación de la prueba de validación.
- Generación y transferencia de la prueba de recepción

Generación y transferencia de la prueba de validación

Se genera una prueba de validación *PV* de la información de resultados intermedios *RI,* que permitirá verificar la identidad de las autoridades electorales que han participado en la generación, validación y envío de dichos resultados. La información de identidad Id_i que se debe incluir en la prueba de validación permite identificar de forma única a cada una de los oficiales de la elección que participan en la generación de dicha prueba. La prueba de validación también permitirá verificar la integridad de los resultados intermedios (i.e., cualquier modificación posterior de la información de resultados intermedios invalidaría la prueba de validación).

La prueba de validación es la concatenación de los resultados intermedios *RI* con el conjunto de identidades de cada uno de los oficiales que participan en su validación. El resultado de dicha concatenación se firma digitalmente como se muestra a continuación:

$$PV = (RI \mid Id_1 \mid Id_2 \mid ... \mid Id_n)_{Sk}$$

La clave *Sk* utilizada para la implementación de esta firma está distribuida entre los oficiales de la elección que participan en la generación de la prueba de validación. En este sentido la clave está custodiada por el conjunto de oficiales de la elección mediante el empleo de un esquema de secreto compartido como el descrito en [Sh79]. Para llevar a cabo la firma digital se define un esquema umbral, en el que no es necesario que participe cada uno de los oficiales a los que se les ha asignado parte de la clave privada, sino que bastará con que un subconjunto predefinido colabora con su parte de la clave. Previamente, la parte de la clave asignada a cada oficial es almacenada en una tarjeta

inteligente protegida por dos parámetros: un PIN (personal identification number) y la huella dactilar del oficial de la elección. Dicha tarjeta es entregada al oficial correspondiente.

La integridad de los resultados intermedios se protege por medio de la firma empleada. Al mismo tiempo, añadiendo la huella dactilar de los oficiales se tiene un control de los que participaron en la validación de los resultados.

Una vez que se ha generado la prueba de validación, se lleva a cabo la transferencia de los resultados intermedios *RI* y de la prueba de validación *PV* a un módulo de consolidación.

Verificación de la prueba de validación

El módulo de consolidación recibe los resultados intermedios y la prueba de validación correspondiente, y verifica que la prueba de validación ha sido generada por los oficiales de elección correctos. Para ello se procede a verificar si la información de identidades (huellas dactilares) contenida en la prueba de validación coincide con las identidades de los oficiales de la elección responsables de realizar esa validación.

Durante esta fase se verifica también la correspondencia de la prueba de validación con los resultados intermedios. Para hacer esto se procede a verificar que la firma digital se corresponda a la información del resultado intermedio recibido.

A partir de estas verificaciones se procede a la aceptación o rechazo de los resultados intermedios recibidos. Si son aceptados se llevará a cabo su consolidación junto con el resto de resultados intermedios recibidos de otras unidades electorales. Además, el módulo de consolidación debe almacenar las pruebas de validación recibidas para ser utilizadas en caso de una auditoria posterior.

Generación y transferencia de la prueba de recepción

Una vez verificada la prueba de validación, el módulo de consolidación genera una prueba de recepción *PR* que contendrá el resultado de la verificación. Este resultado de la verificación contenido en la prueba de recepción puede ser un valor numérico, alfanumérico, un texto o la combinación de estos. Por ejemplo, se podría utilizar un "1" para representar que la verificación ha sido correcta y un "0" en el caso de que sea incorrecta. En el caso de que la verificación sea correcta, la prueba de recepción también contiene una prueba de aceptación generada a partir de la información del resultado intermedio. Esta prueba de aceptación es un hash de la información del resultado intermedio *RI*. Finalmente, el módulo de consolidación firma digitalmente la prueba de recepción. Por ejemplo, la prueba de recepción de unos resultados intermedios recibidos en el módulo de consolidación y validados como "correctos", tendría la siguiente forma:

$$PR = (\text{“1”}, H(RI))_{Sk}$$

La prueba de recepción es enviada a los oficiales de la unidad electoral que corresponda. De este modo, los oficiales de la unidad electoral pueden verificar, a través del hash de *RI*, que los resultados recibidos por el módulo de consolidación corresponden a los que ellos han validado previamente. Además, la prueba de recepción servirá a los oficiales para verificar que esos resultados intermedios se incluyen correctamente en la consolidación y escrutinio global de los resultados. En la figura 7.2 se muestra un ejemplo con niveles intermedios de consolidación.

En los casos en los que se requiera tener un acta oficial impresa con los resultados de la unidad electoral, se podría utilizar la información de la prueba de recepción para proteger de manipulaciones dichas actas. La prueba de recepción se imprime como parte del acta oficial. De este modo, al verificar la existencia de la prueba de recepción en el acta, se puede comprobar que los resultados contenidos en el acta han sido transferidos y aceptados por el módulo de consolidación. Además, debido a que la prueba de recepción

contiene un hash de los resultados enviados, también se puede verificar la integridad del acta comprobando que los resultados mostrados en ella corresponden a los que contiene la prueba de recepción.

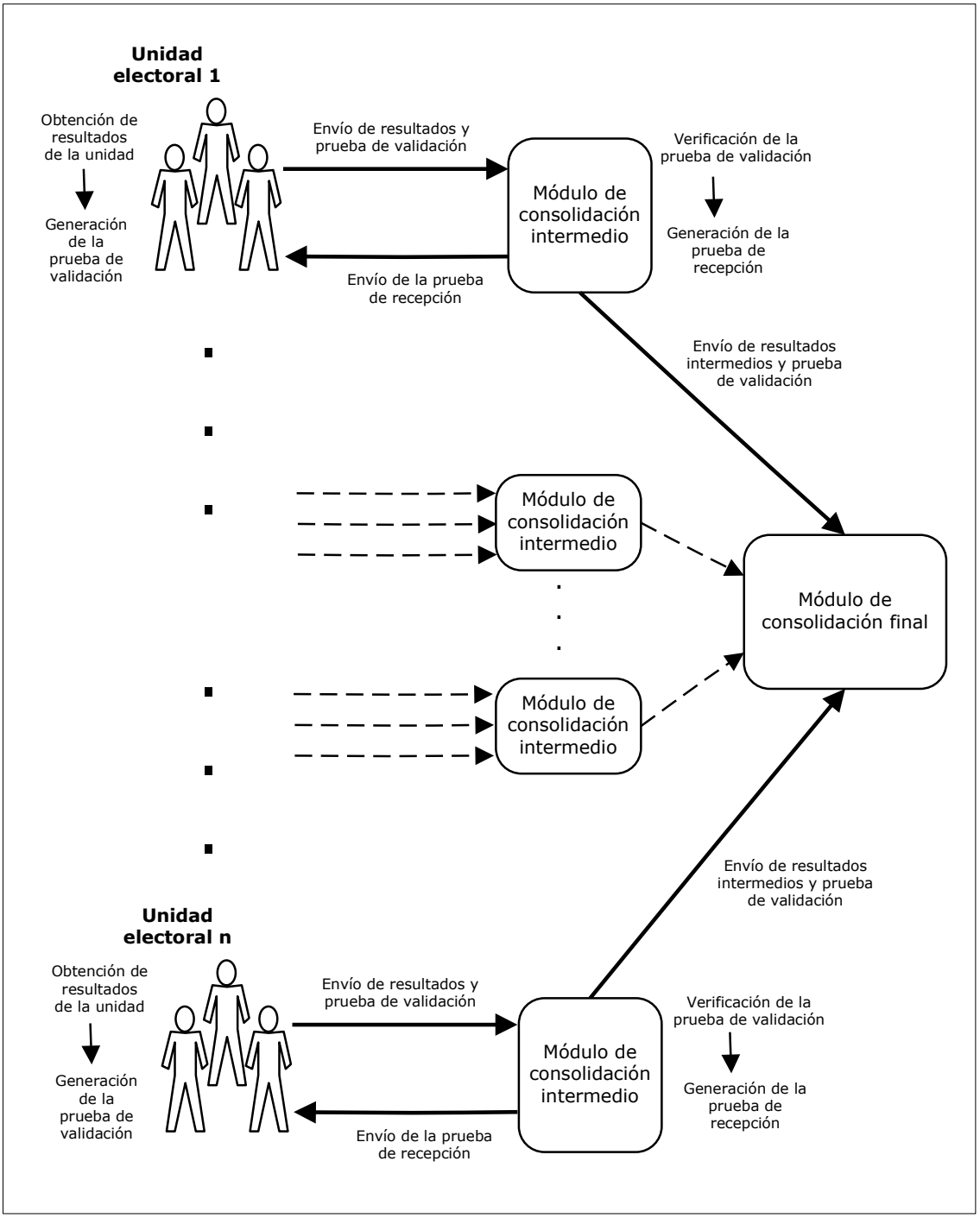

Figura 7.2 Ejemplo del esquema de consolidación de resultados

7.3.2 Pasos finales del proceso de consolidación

Una vez que el módulo de consolidación ha recibido todos los resultados intermedios que le corresponden se lleva a cabo el escrutinio de dichos resultados. Este proceso de consolidación se sigue en cada nivel de consolidación, es decir, si un módulo de consolidación cuenta con un nivel de consolidación superior, entonces debe transferir sus propios resultados intermedios a ese módulo de consolidación superior. Cuando se haya efectuado la consolidación en todos los niveles, se tendrá la representación total de los votos emitidos en la elección, por lo que se puede llevar a cabo el escrutinio final para obtener los resultados de la elección. La figura 7.3 resume los pasos del proceso de consolidación.

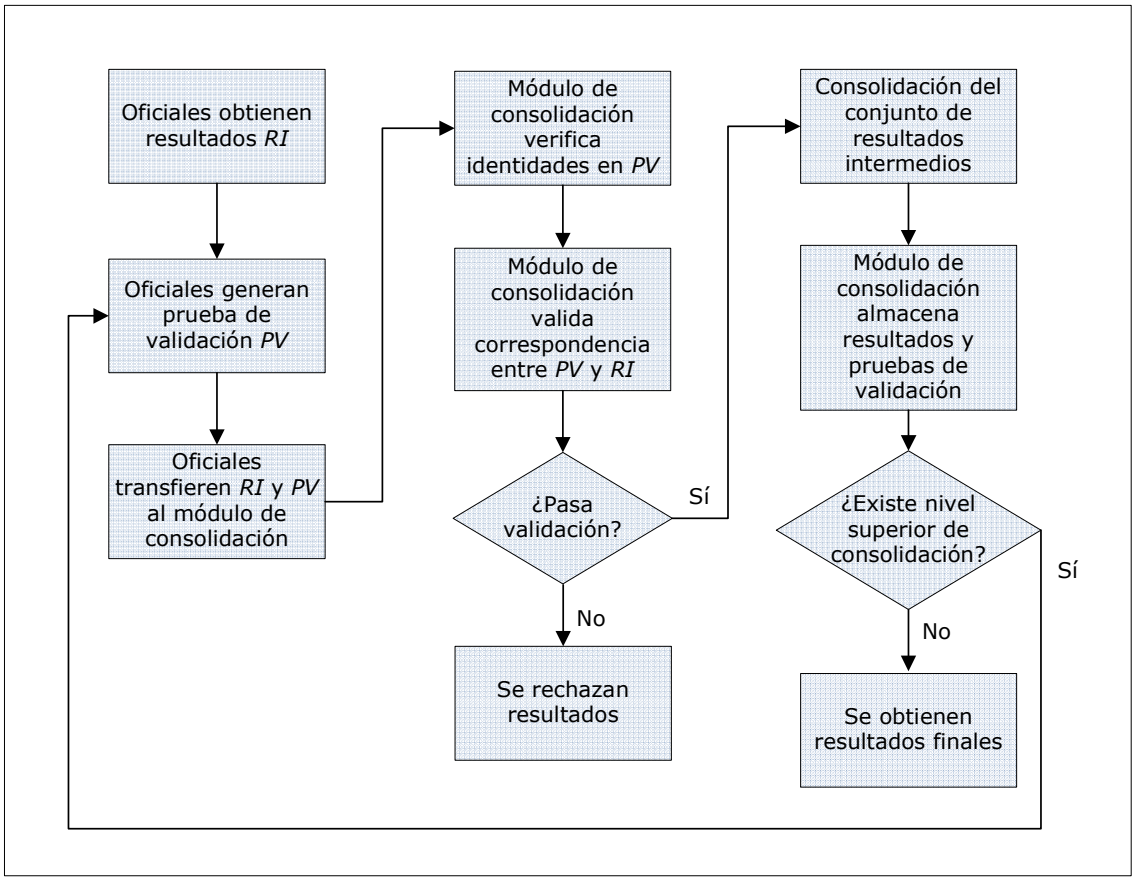

Figura 7.3. Diagrama del proceso completo de consolidación

7.4 Conclusiones y aportación

El esquema descrito en este capítulo facilita la consolidación segura de resultados de un proceso electoral, aplicable tanto a entornos de voto presencial como remoto e incluso a elecciones en las que se utiliza una diversidad de canales de votación de manera simultánea. La consolidación de resultados se lleva a cabo mediante el uso de técnicas y procedimientos que permiten proteger la integridad de los resultados.

El esquema describe diferentes niveles de consolidación. En cada uno de esos niveles se genera una prueba de validación que incluye información de los resultados intermedios y de la identidad de los oficiales de la elección que validaron dichos resultados. De esta manera el módulo de consolidación puede verificar que los resultados recibidos provienen de los oficiales correspondientes a la unidad electoral. Por otra parte, el módulo de consolidación genera y envía a la unidad electoral una prueba de recepción que permite a los oficiales de dicha unidad comprobar que los resultados enviados se han recibido sin ninguna manipulación.

Se ha presentado una solicitud de patente internacional de dicho esquema en dónde se describe una variedad de implementaciones posibles [PMV07b].

Capítulo 8

Auditoria en el Voto Electrónico Remoto

8.1 Introducción

Uno de los desafíos de los sistemas de voto electrónico es ofrecer mecanismos de transparencia que permitan al votante, o a cualquier parte implicada directa o indirectamente en un proceso de elección, verificar la integridad de los resultados. Las propiedades de verificación del votante ampliamente descritas en el capítulo 6, forman parte de la auditoria. Si cada votante verifica el correcto tratamiento de su voto se logra un alto grado de auditoria. Sin embargo hay elementos que quedan fuera del alcance de los votantes. Un ejemplo de esto es la práctica de adición de votos ilegítimos en la base de datos de votos recibidos. En este caso, aún cuando cada votante puede verificar la gestión de su propio voto, ningún votante se percataría de la adición de votos ilegítimos.

En términos generales, la auditoria en un sistema de voto electrónico pretende:

- Comprobar que los votos fueron registrados en el servidor de votación de acuerdo a la elección hecha por los votantes.
- Comprobar que todos los votos registrados fueron correctamente contemplados en el escrutinio final.
- Detectar manipulaciones en cualquiera de los procesos en los que el sistema de votación esté involucrado.
- Detectar errores de funcionamiento en el sistema de votación, los cuáles podrían haber afectado el resultado de la elección.

En los procesos de elección llevados a cabo con sistemas de voto electrónico podemos distinguir dos tipos de auditoria, la que se lleva a cabo antes de la elección y la auditoria posterior a la elección. Además, durante la elección también se llevan a cabo algunas tareas de auditoria por parte del votante. Sin embargo, podemos clasificar dichas tareas como parte de la verificación individual descrita en el capítulo 6, por lo que en este capítulo serán omitidas. En este capítulo se describen diferentes técnicas y procedimientos de auditoria que se utilizan antes y después de un proceso de elección y que pretenden detectar prácticas fraudulentas que puedan alterar el resultado de la elección.

8.2 Auditoria previa a la elección

El objetivo de la auditoria previa a la elección es asegurar que todos los elementos que se usarán en los diferentes procesos funcionan de acuerdo a las especificaciones. Se llevan a cabo verificaciones que a su vez servirán para llevar a cabo auditorias posteriores. De manera más específica, las tareas realizadas en una auditoria previa a la elección son las siguientes:

- *Auditoria de la seguridad*. Se lleva a cabo un análisis exhaustivo de la arquitectura y funcionalidad del sistema de votación con el fin de determinar su seguridad. Este análisis puede incluir una estimación de riesgos y la manera en que el sistema utilizado puede afrontarlos.
- *Verificación de componentes.* Se verifica la integridad de los componentes físicos y lógicos que se utilizarán en la elección.
- *Validación de la configuración de la elección*. Por una parte, se valida que la información que se utilizará para la configuración de la elección (por ejemplo nombres de candidatos, partidos, etc.) corresponde al objetivo de la elección. Además, se verifica que los componentes que se utilizarán corresponden a los que se han validado previamente.

- *Certificación del código fuente*. En la mayoría de los países con legislación en materia electoral se requiere certificar el software que se utilizará en una elección. Después de la certificación, la autoridad de la elección está a cargo de custodiar el software certificado y de vigilar la instalación de dicho software. Sin embargo, se han presentado diversas ocasiones en las que el software utilizado es diferente al que ha sido certificado. Un ejemplo lo encontramos en [HM03]. La certificación del software es un problema crítico tanto para la autoridad de la elección como para los proveedores del software de votación. Por ejemplo, si una vez que el software ha sido certificado el proveedor detecta algún error de funcionamiento, tendría que volver a certificar el software corregido. Esto tiene como consecuencia costos adicionales para el proveedor del software.

Este tipo de auditoria se puede aplicar tanto a los sistemas de voto electrónico presencial como a los sistemas de voto electrónico remoto.

8.3 Auditoria posterior a la elección

En este caso se pretende verificar el correcto funcionamiento de todas las fases de la elección una vez que esta ha finalizado y en algunos casos incluso durante el proceso de votación.

Tal como se ha descrito en el capítulo 6, uno de los propósitos de los sistemas de verificación independiente propuestos en [VVSG06] es tener un registro adicional que permite llevar a cabo una auditoria del proceso de votación. Sin embargo, como ya se ha mencionado antes, dichos sistemas de verificación son adecuados principalmente para los sistemas de voto electrónico presencial, por lo que podemos descartar su viabilidad para un proceso de auditoria en una elección llevada a cabo a través de un sistema de voto electrónico remoto.

En [NASS07] se describen los diversos procedimientos que se llevan a cabo en cada uno de los estados de los Estados Unidos para realizar auditorias posteriores a la elección. Para un sistema de voto presencial (electrónico o basado en papel) se pueden llevar a cabo auditorias posteriores a la elección como las que se describen a continuación.

8.3.1 Recuento total de votos

En el voto convencional basado en papel, en donde el escrutinio de votos es manual, es muy probable que se presenten errores en los resultados debido a la naturaleza humana de los que llevan a cabo dichos escrutinios. Recientemente, en unas elecciones locales basadas en papel en el condado de Palm Beach (Estados Unidos) se informó que en el primer escrutinio se tenía un total de 102523 votos. Debido a lo igualada que estaba la elección entre dos candidatos se llevó a cabo un recuento total en donde se obtuvieron 99045 votos. Hubo una diferencia de 3478 votos entre el primer y segundo escrutinio, que no se pudo explicar. La parte crítica fue que el candidato declarado como ganador tuvo una diferencia de sólo 60 votos respecto al candidato que terminó en segundo lugar [Pa08].

En el voto electrónico, como es bien sabido, el escrutinio de los votos se lleva a cabo de manera automática como parte de las funciones que lleva a cabo el software del sistema de votación. Por lo tanto, un recuento total de los votos por el mismo medio en principio ofrecerá el mismo resultado que el inicial, ya que el cómputo será invariable.

La auditoria posterior a la elección en un sistema de voto electrónico se puede llevar a cabo siguiendo alguno de los métodos de verificación independiente descritos en el capítulo 6, los cuáles aplican tanto a la verificación individual así como para fines de auditoria (sistemas de verificación directa, sistemas de procesos separados, sistemas de testigos, o sistemas de verificación de cifrado extremo a extremo). Los recuentos de votos a través de los registros originados en el sistema de verificación independiente constituyen un mecanismo común para llevar a cabo auditorias de la elección. Sin embargo, los recuentos presentan una seria deficiencia. Un recuento a través de un medio

independiente puede dar diferentes resultados a los obtenidos en el escrutinio inicial, y usualmente el resultado que se tomaría en cuenta sería el del recuento. Sin embargo, los errores o manipulaciones se pueden presentar tanto en el escrutinio inicial como en el recuento, por lo que no podemos considerar que éste sea un método fiable de auditoria. De hecho, un atacante que desee cambiar el resultado de la elección, tendrá más información para llevarlo a cabo con éxito cuando se realizará un recuento. Supongamos que en el escrutinio de una elección el candidato *A* tiene 2500 votos más que el candidato *B*. El atacante (probablemente con privilegios de acceso) sabrá entonces cuantos votos debe agregar antes de que se lleve a cabo el recuento si desea que el ganador sea el candidato *B*.

Un recuento que ofrezca un resultado diferente pero que conserve al mismo ganador del escrutinio inicial, generalmente no será discutible aún cuando la diferencia en el resultado sea significativa. Por otro lado, tal como se analiza en [YB08], un recuento que arroje un ganador diferente al del escrutinio inicial y para el cuál no se pueda dar una explicación de la razón de las diferencias entre ambos conteos, causará un alto grado de desconfianza entre los votantes.

Además, como ya se ha mencionado en el capítulo 6, los sistemas de verificación independiente afrontan el desafío de escoger acertadamente el registro que será considerado como correcto en caso de discrepancias. En el estado de Nevada, por ejemplo, se llevan a cabo comparaciones entre el registro electrónico y los impresos (generados por un sistema VVPAT) y en caso de que no concuerden los resultados, el registro que se considera válido es el electrónico. El caso contrario se presenta en California, en donde ante la misma situación, el registro válido es el de las papeletas impresas.

8.3.2 Recuento de una muestra de los votos

En el voto convencional en papel así como en los sistemas de voto electrónico que generan un respaldo en papel, tal como los sistemas VVPAT, se pueden llevar a cabo

recuentos parciales de los votos. La decisión de llevar a cabo un recuento total o parcial dependerá usualmente de la legislación aplicable al proceso de la elección, así como de las situaciones particulares que requieran de la auditoria. En algunos países y/o estados se requiere llevar a cabo un recuento parcial como procedimiento ordinario después de cada elección. Estos recuentos normalmente se realizan en proporciones pequeñas. Por ejemplo, en el estado de Colorado se audita el 5 % de las máquinas utilizadas, mientras que en Maryland al menos el 10 % de los recintos deben ser auditados y en Minnesota entre 2 y 4 recintos por condado dependiendo del número de habitantes. En Carolina del Norte, actualmente se audita una muestra de 260 recintos. Para más ejemplos de parámetros utilizados para auditorias se puede consultar [NASS07].

Otras consideraciones importantes para llevar a cabo un recuento parcial como parte de una auditoria, es que por un lado un recuento total de los votos es muy costoso y por otro lado, como ya se ha mencionado antes, existe un riesgo muy alto de que se encuentren diferencias entre el escrutinio original y el recuento, con el impacto que eso puede tener. En cambio, en un recuento menor en dónde se han seleccionado apropiadamente los parámetros para determinar la muestra, se podría tener una idea clara de la fiabilidad del escrutinio original o de la posibilidad de que haya existido fraude. Esto, sin tener que llegar a un nivel alto de precisión requerido en los recuentos totales.

Existen diferentes trabajos basados en procesos estadísticos o probabilísticos que hacen un análisis del porcentaje de votos, de máquinas de votación o de los recintos que deberían ser auditados a fin de detectar con una probabilidad alta si han existido alteraciones en los resultados de la elección [St06, Ri06b, St08a]. Usualmente se toman como variables el número total de recintos o máquinas de votación, el margen de diferencia de votos entre el candidato presumiblemente ganador y el segundo lugar, y el tamaño de los recintos [St08b].

El problema de determinar el número de recintos es menor si consideramos que el problema principal de los recuentos parciales se encuentra en la decisión de cuáles recintos formarán parte del recuento. Si un atacante sabe en cuáles recintos o de cuáles

máquinas de votación o conjunto de votos se llevará a cabo el recuento, y consigue acceso a dichos elementos entonces podrá tomar ventaja añadiendo o eliminando votos de acuerdo con su interés. Si a esta situación añadimos que la decisión de los recintos que serán auditados se puede conocer antes del cierre de la elección, un atacante podrá manipular uno o más recintos de los que no se han considerado para ser auditados y esto no será detectado.

En [CWD06] se define un método de selección de recintos basado en dados de 10 caras. Para empezar, a cada unidad sujeta a auditoria (recinto, máquina de votación, Etc.) se le asigna un número secuencial que identificará a dicha unidad. Cada una de las caras de un dado representa los dígitos correspondientes a las unidades, decenas, centenas, millares, etc. El dado que representa las unidades tendrá en sus caras los dígitos 0, 1, 2, … ,9. El que representa las decenas tendrá en sus caras 00, 10, 20, …,90, y así sucesivamente hasta cubrir el total de recintos. Por ejemplo, si tenemos 500 recintos se requieren 3 dados, y si tuviéramos 5000 recintos se requerirían 4 dados para cubrir todos sus dígitos. Entonces se lleva a cabo el lanzamiento de dados un número de veces correspondiente al número de unidades que se pretenden auditar. Este método es eficiente si consideráramos que todos los recintos tienen el mismo tamaño. Sin embargo esta circunstancia no será muy común. En [APR08] se añade como una variable el tamaño de los distintos recintos para determinar la muestra a auditar, lo cuál aumenta la eficiencia al escoger recintos en donde existe una mayor probabilidad de que un fraude pueda afectar el resultado de la elección. Por otro lado, la tarea de determinar los recintos a auditar se vuelve más compleja entre mayor es el número de recintos.

Otros trabajos consideran que la mejor forma de decidir cuál será la muestra a auditar es por medio de funciones pseudo-aleatorias. Ver por ejemplo [Ri08, CHF08]. Estas técnicas implican menos trabajo y tiempo por parte de los involucrados en el proceso, sin embargo, podrían incumplir con la transparencia del proceso de selección de la muestra a auditar.

En [CHF08 y CWD06] se definen las propiedades que debe tener toda muestra de votos escogida para una auditoria:

- No predecible. Un adversario no debe tener la posibilidad de saber o predecir con certeza cuál será la muestra a auditar, ya que el tener conocimiento de ello representa una ventaja para llevar a cabo manipulaciones no detectadas.
- Verificable. Los ciudadanos deben tener confianza (mediante alguna verificación) en que la muestra elegida para auditoria no ha sido escogida de manera premeditada o que de alguna manera ha habido manipulaciones para su selección.
- Robusta. El hecho de que al menos uno de los participantes en el proceso de selección de la muestra a auditar es honesto debe ser suficiente para que se confíe en dicho proceso.
- Simple. El proceso de selección de la muestra de auditoria debe ser lo suficientemente simple como para que todos los participantes en el proceso de selección lo puedan entender.
- Eficiente. La selección de la muestra debe cumplir con el propósito de la auditoria.

En general los recuentos de votos, ya sea de manera parcial o total, permiten detectar irregularidades en el escrutinio inicial, sin embargo no es posible detectar los problemas de manipulación de votos que se pueden llevar a cabo antes del escrutinio inicial o incluso las manipulaciones que pueda haber en los períodos intermedios entre un conteo y otro.

Para llevar a cabo una auditoria posterior a la elección en un sistema de voto electrónico remoto no se pueden considerar las mismas técnicas y métodos utilizados en los sistemas de voto presencial. A fin de detectar manipulaciones en los resultados de la elección en los sistemas de voto electrónico remoto, es necesario llevar a la práctica nuevos mecanismos de auditoria que satisfagan los requerimientos de seguridad y las particularidades de dichos sistemas. A la fecha se han propuesto algunas técnicas criptográficas que ayudan en la detección de manipulaciones, tales como el uso de un tablón de anuncios electrónico (EBB) o sistemas de protección de logs.

8.3.3 Tablón de anuncios electrónico (EBB) para auditoria

Se ha propuesto en diversos trabajos el uso de un tablón electrónico, como el descrito en el capítulo 6, como un mecanismo permite llevar a cabo auditorias de la elección. Un tablón electrónico además de servir para que el votante pueda verificar su propio voto, permite la verificación universal y por lo tanto la posibilidad de auditoria.

Un ejemplo de este grupo de propuestas es el sistema Helios [Ad08]. Helios es un protocolo para votación y auditoria pública (verificación universal) que funciona a través de una interfaz Web y está basado en [Be06]. El protocolo utiliza el criptosistema ElGamal [El84] para llevar a cabo el cifrado de los votos y funciona de la siguiente manera:

1. El votante accede a la plataforma de votación sin necesidad de autenticarse, entonces escoge y cifra su voto y se genera un recibo de votación, el cuál es un hash del voto cifrado.

2. Antes de que el voto sea enviado, se le pregunta al votante si desea enviarlo o utilizarlo para auditoria.

3. Si el votante decide auditar el voto, se le revela el factor de aleatoriedad utilizado para cifrar su voto. Entonces el votante puede verificar que el voto cifrado corresponde a la selección que había realizado. Debido a que el voto ha sido abierto para ser auditado, el votante debe iniciar otra vez el proceso de votación si quiere enviar el voto.

4. Si el votante escoge enviar su voto, se le piden sus credenciales de votante para llevar a cabo la autenticación.

5. Los votos cifrados y enviados por los votantes son publicados en tiempo real en el tablón electrónico junto al nombre o un identificador del votante. De esta forma, cada votante puede verificar que su voto ha sido recibido y publicado.

6. Auditores o cualquier parte interesada puede acceder al tablón de anuncios y descargar los contenidos a fin de verificar el correcto tratamiento de los votos.

Aún cuando un tablón de anuncios electrónico es una buena forma de auditar el correcto tratamiento de los votos, se requiere de un mecanismo adicional que permita romper la relación del voto con el votante que lo emitió. En el sistema Helios esto se lleva a cabo utilizando una mix-net de re-cifrado. Como se describe en el capítulo 4, el uso de una mix-net a su vez requiere de elementos que permitan verificar su correcta operación, por ejemplo la implementación de pruebas de conocimiento nulo que resultan muy costosas computacionalmente, especialmente si se trata de una elección a gran escala.

8.3.4 Sistemas de protección de logs

Un log es un registro de eventos que suceden en un período específico. El log usualmente registra información sobre un evento y la fecha en que el evento ha ocurrido. En una forma más extensa, el log representa el ¿quién?, ¿qué?, ¿cuándo?, ¿dónde? y ¿porqué? de un evento que ha ocurrido en un dispositivo o aplicación.

En los sistemas de voto electrónico se suele llevar un registro de los eventos generados en la elección a fin de tener evidencias de lo que ha sucedido en caso de que se dude o se sospeche de la integridad de una elección. Por ejemplo, en una sesión de voto se generará el registro del evento de autenticación del votante, la selección de candidatos, la confirmación de candidatos, el cierre de sesión, etc.

Debido a que los logs contienen los eventos que suceden en la elección, un atacante que ha manipulado una elección podría también tratar de manipular los logs generados para eliminar el rastro del ataque. Para mantener los logs seguros, es necesario contar con

técnicas de prevención y detección de manipulaciones. Para detectar manipulaciones en los logs se han propuesto diferentes métodos. Los métodos más importantes para la protección de los logs son descritos a continuación.

En [BY97] se introduce el concepto de "forward integrity", el cual consiste en que aún cuando los logs se vean comprometidos por un atacante, éste no pueda manipular los contenidos que forman los logs hasta ese momento. Los contenidos podrían ser eliminados, sin embargo, esto debería ser detectado. El trabajo en [BY97] hace uso de funciones MAC (códigos de autenticación de mensajes) para proteger los logs. En un contexto de comunicación remota, el uso de una función MAC se utiliza teniendo una clave privada la cuál es compartida solamente entre el emisor y el receptor. El emisor del mensaje usa dicha clave privada para generar un MAC del mensaje y entonces envía el mensaje junto con su correspondiente MAC. Ya que el receptor conoce la clave privada, aplica la misma función sobre el mensaje original para generar el MAC. A continuación, el receptor compara el MAC recibido con el MAC generado. El receptor sabrá que el mensaje no ha sido alterado si ambos MAC coinciden. La seguridad de este esquema se basa en que es computacionalmente inviable que un atacante que no conoce la clave privada modifique el mensaje y que cuando el receptor compare los MAC´s resulte una coincidencia entre ambos. Debido a que los logs son simples mensajes generados durante cierto período de tiempo, y que en algún momento son leídos y verificados por un auditor, sería eficiente que la protección de los logs se llevara a cabo aplicando una función MAC sobre ellos. Sin embargo, el problema es que si un atacante consigue la clave privada entonces podrá modificar los logs sin ningún riesgo de ser detectado. En dicho trabajo también se describe cómo se puede evitar que un atacante que se apodera de la clave privada en cierto momento, manipule los logs generados antes de ese momento. Esto se logra haciendo que la clave privada usada para general el MAC evolucione a través del tiempo. La clave privada k_i en un tiempo t_i se obtiene aplicando una función unidireccional a la clave k_{i-1} que pertenece a un tiempo previo t_{i-1} y una vez iniciado el tiempo t_i, la clave k_{i-1} es eliminada. De esta manera, si el atacante obtiene la clave privada k_i, no podrá saber nada acerca de una clave privada k_j para $j < i$. Por lo tanto, los logs originados antes del compromiso de la clave privada no pueden ser modificados.

El esquema descrito previamente presenta algunos inconvenientes. Si un atacante logra comprometer una clave k_i, entonces el mismo atacante podría ser capaz de comprometer una clave k_{i-1} y cualquier otra clave privada utilizada en el esquema. Por otro lado, la complejidad en la administración de las claves privadas aumenta conforme aumenta la cantidad de claves. Un auditor debería usar entonces n claves privadas para verificar la integridad de los logs. Una propuesta similar sería utilizar firmas digitales en lugar de funciones MAC. Esto reduciría el problema de la gestión de las claves que se puede dar en el esquema anterior.

Un esquema criptográfico de protección de logs como el descrito previamente, sólo contempla los ataques en los que los logs pueden ser modificados. Sin embargo, en dicho esquema no se considera que los logs también podrían ser eliminados.

En [SK98] se propuso un protocolo de protección de logs. En este protocolo se consideran tres agentes: una máquina insegura, una máquina segura y el verificador (o auditor). La máquina insegura es donde se generan los logs. El propósito es que los logs se vayan replicando a través del tiempo o cuando se alcance cierto número de eventos. Dicha réplica se haría en la máquina segura a través de una red de datos. El protocolo utiliza una combinación de funciones hash, firmas digitales y criptografía de clave pública y privada. Este protocolo, al igual que el descrito en [BY97], aborda el problema de la protección de los logs generados antes del compromiso de los mismos.

Propuestas más recientes de protección de logs y que además son orientadas a voto electrónico son los trabajos presentados en [RP04 y SDC+08]. En [RP04] se establece un protocolo de protección de logs como parte de un sistema de voto electrónico remoto. Para cada log individual se va calculando en tiempo real un valor hash. Además, se utiliza un algoritmo de firma digital periódica, es decir, se lleva a cabo una firma cada vez que se acumula cierto número de logs (un bloque predeterminado) o en su defecto cada cierto tiempo. Los logs individuales se van encadenando con los logs generados previamente, de la siguiente manera:

$$\dots$$
$$L_i = \mathrm{H}(l_i \mid L_{i-1})$$
$$L_{i+1} = \mathrm{H}(l_{i+1} \mid L_i)$$
$$L_{i+2} = \mathrm{H}(l_{i+2} \mid L_{i+1})$$
$$L_{i+3} = \mathrm{H}(l_{i+3} \mid L_{i+2})$$
$$\dots$$

En donde l es un log individual y L es el resultado de aplicar una función hash a la concatenación de l con el L previo.

Una vez que se ha completado un bloque b_i de logs de tamaño predeterminado se lleva a cabo la firma digital de dicho bloque:

$$Sig_i = [\mathrm{H}\ (b_i \mid sig_{i-1})]S_k$$

En donde S_k es la clave privada del servidor a cargo de firmar los logs. La clave pública servirá para verificar la integridad de dichos logs.

Por medio de este protocolo se forma una cadena de integridad entre los logs. Si un atacante modifica los logs, será detectado cuando se lleve a cabo la verificación de las firmas. Por otro lado, si un log es eliminado, también puede ser detectado cuando se lleve a cabo la verificación del bloque al que pertenecía.

Es importante notar que para un auditor puede resultar muy complejo llevar a cabo un análisis de los logs cuando la cantidad de eventos registrados es muy grande. Esta complejidad tiene como consecuencia la dificultad de lograr la detección de manipulaciones. Por ejemplo, en un ataque de “stuffing” en el cuál los votos ilegítimos son añadidos directamente en la base de datos en dónde se almacenan los votos, el auditor sólo podría detectarlo si extrae de los logs la cantidad de votos que se recibieron durante la etapa de votación y compara esa cantidad con la de los votos contabilizados para generar el resultado de la elección. Suponiendo que se han recibido un millón de votos, y

que por cada voto emitido se generan varios logs, tendremos entonces unos cuantos millones de logs que se deben analizar.

En [SDC+08] se describe una herramienta llamada "Querifier", que permite analizar de manera automática y en tiempo real, los eventos (logs) generados en un sistema. Dicha herramienta pretende evitar la complejidad que supone llevar a cabo el análisis de logs. El mecanismo se basa en un conjunto de reglas definidas con lógica de predicados. Estas reglas determinan los eventos posibles en el sistema y el orden en que pueden suceder dichos eventos. Para saber si un evento cumple o viola alguna de las reglas se lleva a cabo un análisis sintáctico del log. Entonces se determina su validez. El mecanismo también detecta si se ha roto la cadena de hash generados para proteger la integridad de los logs. De esta manera se puede conocer el momento y las circunstancias en que se ha llevado a cabo algún ataque o intento de corrupción en el log. Como ejemplo de las reglas definidas para el sistema de votación electrónica, un evento de "voto registrado" debería estar precedido por el evento de "votante autorizado", de otra manera el sistema detectaría que ha habido alguna corrupción de eventos.

Teniendo en cuenta los aspectos contemplados en los esquemas ya descritos para llevar a cabo auditorias eficientes en los sistemas de voto electrónico remoto, podemos concluir que la mayoría de estos esquemas basan la detección de manipulaciones en el análisis de los logs generados. De acuerdo a los esquemas descritos, la parte más compleja, además de la protección de los logs, es la verificación de integridad que deben llevar a cabo los auditores. En la siguiente sección se presenta una propuesta de auditoria para sistemas de voto electrónico remoto.

8.4 Propuesta de auditoria mediante resúmenes de votación

Los actores que podrían participar en un ataque de adición de votos ilegítimos pueden ser atacantes externos, los cuáles requieren quebrantar las medidas de seguridad establecidas para proteger la base de datos, o bien, podrían ser autoridades de la elección o personal

técnico con privilegios de acceso a los elementos de la elección. Por esta razón, no podemos asumir que sería suficiente establecer un control de acceso en la base de datos para evitar que se lleven a cabo manipulaciones. En esta propuesta se considera una contramedida para el ataque de adición de votos por parte de un atacante interno con privilegios de acceso a los elementos de la elección.

Se propone un mecanismo de auditoria que tiene como finalidad detectar las prácticas de adición de votos ilegítimos. El objetivo principal de dicha propuesta es ofrecer un mecanismo que resulte fácil de implementar, es decir, que facilite la tarea de llevar a cabo una auditoria a fin de detectar las prácticas fraudulentas mencionadas previamente.

La propuesta se basa principalmente en una técnica de protección de los votos individuales que permite llevar a cabo auditorias a un nivel más alto que el análisis de logs, y por lo tanto con menor complejidad. El propósito es generar lotes de respaldo de los votos a medida que estos se van recibiendo en el servidor de votación. Cada cierta cantidad de votos recibidos se concatenan y son firmados por una autoridad o conjunto de autoridades con la clave *Sk*, lo cuál forma un lote *L*:

$$L = \{V_1 \mid V_2 \mid V_3 \mid \ldots \mid V_n\}_{Sk}$$

Por ejemplo, si se determina que los lotes deben contener 100 votos, estarían formados de la siguiente manera:

$$L_1: \{V_1, \ldots, V_{100}\}_{Sk}$$
$$L_2: \{V_{101}, \ldots, V_{200}\}_{Sk}$$
$$\ldots$$
$$L_n: \{V_{100n-99}, \ldots, V_{100n}\}_{Sk}$$

Estos lotes de votos firmados se almacenan en un servidor diferente al de voto, o bien, en algún medio de almacenamiento extraíble. La firma digital de los lotes asegura que si se presenta una manipulación en alguno de los lotes pueda ser detectada. Sin embargo, un

atacante podría añadir nuevos lotes y si posee la clave privada podría firmarlos. Este ataque ocasionaría que si se lleva a cabo una auditoria no concuerden los votos contabilizados originalmente con los votos respaldados en lotes. A fin de prevenir este ataque, se forma una cadena de integridad de los lotes a medida que se van generando. Esta cadena de integridad se realiza llevando a cabo un hash de la concatenación del lote anterior firmado con el lote actual también firmado:

$$L'_1 = \mathrm{H}\,[L_1]$$
$$L'_2 = \mathrm{H}\,[L'_1 \mid L_2]$$
$$\dots$$
$$L'_n = \mathrm{H}\,[L'_{n-1} \mid L_n]$$

En caso de una auditoria, es necesario contar con un identificador único de voto para poder relacionar los votos contenidos en los lotes con los votos almacenados por el servidor de votación. El identificador de voto también sirve para formar los lotes de respaldo de acuerdo a la unidad electoral a la que pertenecen si esto se considera necesario, por ejemplo a un municipio, provincia, distrito electoral, etc. Este identificador se debe generar durante la fase de votación y se compone por ejemplo de un grupo de dígitos que indican la unidad electoral y el siguiente grupo que consiste en un número secuencial. Por ejemplo, el identificador "036408475" representa que el voto pertenece a la unidad electoral 0364 y que es el voto secuencial número 08475. La generación de un identificador de voto solamente se debe llevar a cabo durante una sesión de voto una vez que el votante ha sido autenticado. De esta manera, si se añaden votos ilegítimos directamente en la base de datos no se contará con un identificador válido.

La práctica fraudulenta de adición de votos ilegítimos se puede presentar en tres períodos: antes de dar inicio a la votación, durante la fase de votación o, una vez concluida dicha fase. La adición de votos antes del inicio de la fase de votación se puede detectar fácilmente con procedimientos de verificación, por ejemplo, asegurándose que la base de datos en donde se almacenarán los votos esté vacía justo antes de que inicie la

votación. Por su parte, la adición de votos durante la fase de votación o al término de la misma puede detectarse con el esquema propuesto, tal como se explica a continuación.

Si al terminar la fase de consolidación se requiere realizar una auditoria de los resultados de votación, se llevan a cabo una serie de validaciones mediante la comparación de los votos incluidos en el escrutinio con los votos contenidos en los lotes de respaldo. La figura 8.1 muestra el esquema propuesto de manera general.

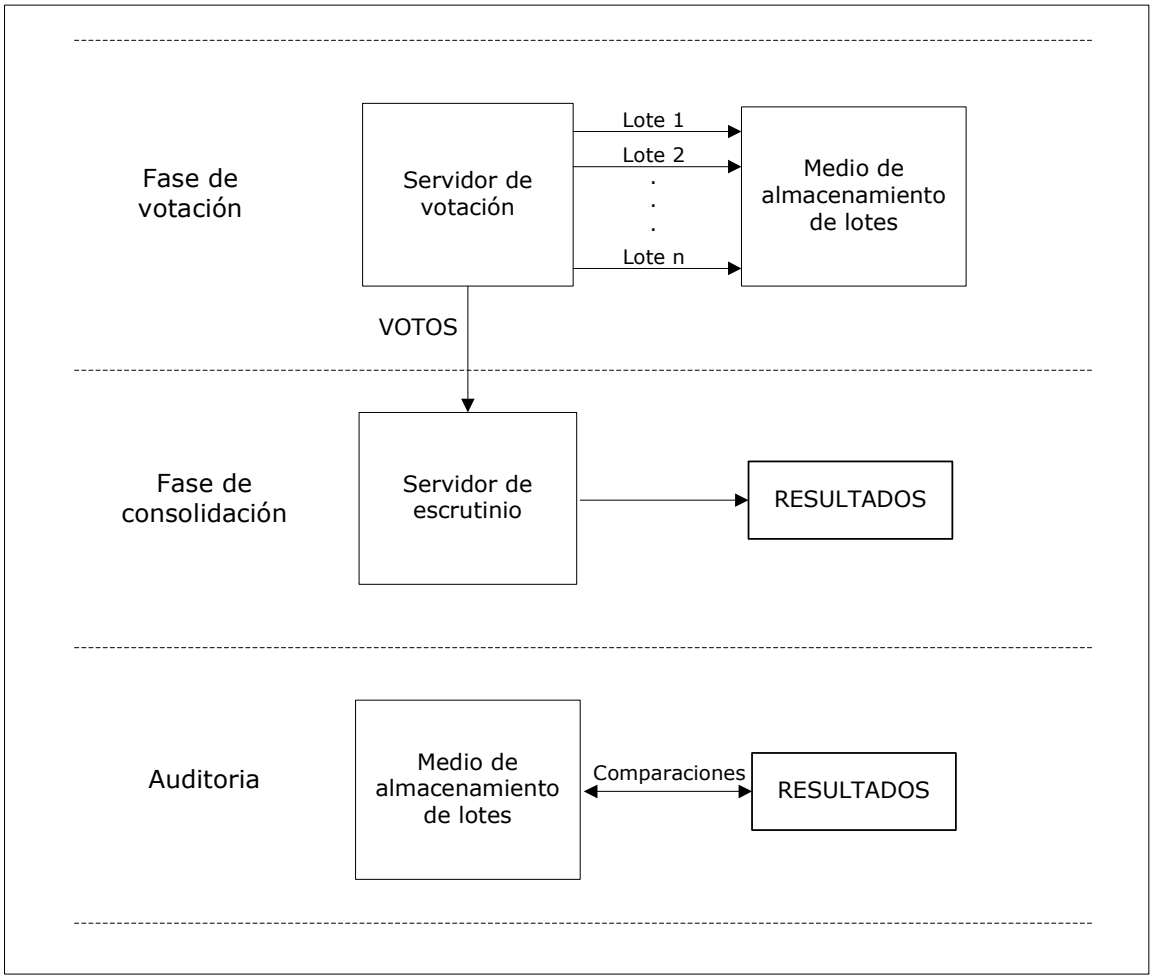

Figura 8.1. Esquema de auditoria

Las validaciones de la auditoria se llevan a cabo en el siguiente orden:

1. Se verifica la integridad de los lotes. Esto se lleva a cabo revisando la cadena de integridad de los lotes y la firma digital en cada uno de ellos.

2. Se compara el número de votos incluidos en el escrutinio con el número de votos en los lotes de respaldo. Si el número de votos que se incluyeron en el escrutinio es mayor que el de votos contenidos en los lotes se puede saber que se han añadido votos ilegítimos. Aún así se debe realizar el siguiente paso para detectar cuáles son los votos que se han añadido.

3. En base al identificador de voto, se verifica que cada voto incluido en el escrutinio se encuentra también en alguno de los lotes. Los votos del escrutinio cuyo identificador no coincida con alguno de los votos registrados en los lotes de respaldo se catalogan como votos ilegítimos.

Al llevar a cabo estas validaciones se puede saber con certeza si han sido añadidos votos ilegítimos en la base de datos original e incluso se pueden detectar cuáles han sido esos votos. Si es necesario, se lleva a cabo un nuevo escrutinio de los votos. El encadenamiento de los lotes que se almacenan en el servidor externo o medio extraíble permite detectar cualquier manipulación que atente con la integridad de dichos lotes.

Este tipo de auditoria se puede aplicar también antes de realizar el escrutinio de votos. Como se ha mencionado previamente en este capítulo, en algunas elecciones se debe llevar a cabo como regla una auditoria de un porcentaje de los votos. En un caso como éste se seleccionan, de manera aleatoria, grupos de votos (en base al porcentaje que se requiera auditar) y los lotes de respaldo correspondientes. Los grupos de votos seleccionados pueden por ejemplo pertenecer a una unidad electoral. Debido a que los votos que están almacenados en el servidor de votación cuentan con un identificador, la selección que se haga de los grupos de votos a verificar se podrá hacer corresponder sin ninguna dificultad con los lotes de respaldo formados durante la votación. Por ejemplo, si los lotes son de 100 votos y los grupos de votos a verificar son el 5, 9, 16, 31 y 37, se compararán los votos del 501 al 600, del 901 al 1000, del 1601 al 1700, del 3101 al 3400

y del 3701 al 3800 con los lotes que contienen dichos votos. La verificación se lleva a cabo comparando los identificadores del grupo y del lote. Para determinar el número de lotes a verificar mediante esta técnica, se deben considerar los parámetros adecuados para que se pueda detectar con una probabilidad alta si se han añadido votos ilegítimos. Dado que este tipo de auditoria se lleva a cabo cuando los votos se encuentran cifrados, no existe ningún riesgo de violar la privacidad de los votantes.

Este método de respaldo y comprobación de lotes se puede aplicar a diferentes esquemas de votación. En esquemas de votación en donde los votos se cifran del lado del votante, los lotes se pueden ir formando conforme los votos son recibidos en el servidor de votación. Por su parte, en esquemas de papeletas precifradas, como el propuesto en el capítulo 6, los lotes son formados por los códigos de votación cuando son recibidos y cifrados por el servidor de votación.

Al llevar a cabo una auditoria como la descrita previamente se pueden encontrar irregularidades que requieran un análisis mayor que el proporcionado por el esquema propuesto. Si se presenta un caso que lo requiera, se debe pasar a un nivel de auditoria más bajo, por ejemplo a través del análisis de logs, como ha sido explicado previamente en este capítulo.

8.5 Conclusiones y aportación

En este capítulo se han analizado los métodos de auditoria para los diferentes sistemas de votación. Se ha descrito la forma en que los sistemas de verificación independiente podrían facilitar la auditoria de un sistema de voto electrónico presencial. En cambio, en un sistema de voto electrónico remoto resulta inviable hacer uso de alguno de los sistemas de verificación independiente. Tal como se ha descrito en el capítulo 6, el registro de respaldo generado por un sistema de verificación independiente tiene dos propósitos: i) que el votante pueda verificar que su voto se ha registrado correctamente y ii) tener un registro independiente del sistema de votación que pueda usarse para fines de

auditoria. En un ambiente remoto de votación no se puede cumplir con ambos propósitos. Si el registro independiente se genera del lado del votante para que este pueda verificarlo, entonces dicho registro no lo tendrá la autoridad de la elección, lo que descarta la posibilidad de usar el sistema de verificación independiente como mecanismo de auditoria. Por otro lado, si el registro independiente se enfoca solamente a la auditoria llevando a cabo un registro independiente centralizado, existe el riesgo de violación de la privacidad del votante o de generación de registros independientes que no coincidan con los votos reales. Por ejemplo en una votación por Internet, si además de registrarse el voto cifrado en un servidor de votación se imprime una papeleta en un centro de impresión custodiado por la autoridad de la elección, el votante puede perder su privacidad ya que se puede relacionar con la opción de voto escogida. Además, el voto impreso puede ser diferente al enviado por el votante y esto no podría ser detectado al menos durante la elección.

Los sistemas de voto electrónico remoto pueden ser auditados a través de los logs de eventos registrados durante el proceso de votación. Sin embargo, como ya se ha explicado en este capítulo, la administración y auditoria de logs presenta algunos retos importantes para llevar a cabo su análisis.

Se ha descrito en este capítulo un mecanismo que permite la detección de ataques en los que se añaden votos de manera ilegítima para ser parte del escrutinio. En el capítulo 6 se describió la manera en que los votos, de manera individual, pueden ser verificados por los votantes con el fin de asegurar que dichos votos se incluyen correctamente en el escrutinio. Con dichas verificaciones se puede detectar si se han eliminado o manipulado votos legítimos. Por su parte, en este capítulo se ha descrito una forma de verificar que en el escrutinio solamente se han incluido los votos que se han emitido por votantes legítimos. Por lo tanto, esta propuesta y las técnicas de verificación individual presentadas en el capítulo 6, permiten ofrecer la transparencia que necesita un sistema de voto electrónico remoto. Esta transparencia es indispensable para que un sistema de votación sea fiable para todos los participantes en la elección, es decir, votantes, autoridades de la elección, candidatos, etc.

Capítulo 9

Conclusiones

El principal objetivo de la investigación presentada en esta tesis ha sido el estudio de mecanismos que proporcionan seguridad y transparencia a los diferentes procesos de las elecciones que hacen uso del voto electrónico remoto. El criterio principal para la selección de las áreas de estudio ha sido la necesidad de generar mayor confianza en los sistemas de voto electrónico remoto. Cada una de las propuestas presentadas pretende aportar mecanismos que ayuden a la fiabilidad de dichos sistemas, desde el punto de vista de los votantes así como de otros participantes de la elección.

En el capítulo 1 se describieron los principales conceptos relacionados con elecciones y la forma en que se ha tratado de hacer más eficiente cada uno de los procesos involucrados en una elección. También se presentaron algunas de las experiencias de voto electrónico remoto que se han llevado a cabo alrededor del mundo y los retos que dichas experiencias han afrontado. Finalmente, se definieron los problemas que se ha considerado son los más críticos en el desarrollo del voto electrónico remoto.

En el capítulo 2 se presentaron los conceptos básicos de criptografía aplicada al voto electrónico. El propósito de este capítulo ha sido ayudar al lector a comprender mejor cada uno de los protocolos criptográficos presentados a lo largo de la tesis.

En el capítulo 3 se presentaron los diferentes sistemas de voto remoto, incluyendo el voto postal, el cuál es actualmente el más utilizado. Se ha llevado a cabo una comparativa del voto postal y los diferentes sistemas de voto electrónico remoto. Esta comparativa tiene la

finalidad de evaluar las ventajas que proporcionaría el uso de un sistema de voto electrónico remoto en comparación con el actual sistema de voto postal. Se puede concluir que entre los sistemas de voto electrónico remoto, el voto por Internet es el más adecuado para sustituir al voto postal, debido principalmente a ciertas ventajas de seguridad, por ejemplo: mayor facilidad para la autenticación del votante, garantía de equidad para los votantes, precisión en el escrutinio y verificación del correcto tratamiento de los votos. Además, sobresalen las características de usabilidad del voto por Internet, como la prevención de errores involuntarios al seleccionar el voto o la facilidad que se ofrece a los votantes con alguna discapacidad visual para llevar a cabo la selección y envío de su voto sin asistencia de terceros. En el capítulo se mostró una comparativa de diferentes sistemas de voto remoto. Esta comparativa de sistemas de votación fue presentada en Bochum, Alemania en la conferencia "E-Voting and Identity" y publicada en [PM07b].

En dicho capítulo también se llevó a cabo un estudio de las vulnerabilidades y amenazas de los sistemas de voto electrónico remoto, de manera más específica, en el voto por Internet. El conjunto de vulnerabilidades y el catálogo de amenazas presentados es parte de un análisis de seguridad llevado a cabo para un proyecto piloto que se realizó para las elecciones presidenciales de los Estados Unidos en Noviembre del 2008. En dicho piloto, militares pertenecientes al condado de Okaloosa, Florida, que residen en tres bases militares ubicadas en el Reino Unido, Alemania y Japón utilizaron un sistema de voto por Internet desarrollado por la empresa "Scytl Secure Electronic Voting". El resultado de dicho análisis es parte de un informe técnico de dicha empresa [Sc08b].

En el mismo capítulo se describió un esquema de votación que pretende ser la base para una transición hacia el voto remoto por Internet. El esquema ha sido publicado en el IJEG (International Journal of Electronic Governance). Véase [MSM+08] para los detalles de la publicación. Considerando los elementos que se utilizan en este esquema, como son la tarjeta de votación, y la posibilidad de diversos canales simultáneos de votación, se contribuye a la evolución hacia el uso extensivo del voto electrónico remoto. La tarjeta de votación, la cuál está basada en una tarjeta inteligente en red, junto con el

requerimiento de la huella dactilar del votante permite llevar a cabo una autenticación robusta de votantes. El esquema reduce en gran manera la posibilidad de coerción o venta de votos. Primeramente, debido a la baja probabilidad de usurpación de la identidad durante la sesión de voto. Por otro lado, la posibilidad de múltiple voto también contribuye a disminuir la coerción, ya que el votante tiene la posibilidad de enviar un nuevo voto si ha sido coaccionado.

En el capítulo 4 se analizaron los diferentes grupos de esquemas criptográficos utilizados en el voto electrónico. Cada uno de esos grupos de esquemas tratan los requisitos de seguridad en distintas maneras, sin embargo, la principal aportación de los tres primeros (firma ciega, mix-nets y cifrado homomórfico) es la forma en cómo logran satisfacer el requisito de privacidad. Los esquemas de firma ciega, tal como se ha analizado, tratan de proteger la privacidad de los votantes al separar las entidades de autenticación y recepción del voto. Los esquemas basados en mix-nets abordan el problema de la privacidad llevando a cabo una serie de transformaciones de los votos (cifrados y permutaciones) para eliminar la relación entre votos y votantes. Por su parte, los esquemas basados en cifrado homomórfico utilizan las propiedades homomórficas de algunos criptosistemas que permiten obtener los resultados de la elección sin la necesidad de descifrar los votos individualmente, protegiendo de esta forma la privacidad de los votantes. Sin embargo, los tres esquemas presentan el riesgo de que un voto pueda ser conocido por un atacante, e incluso manipulado, en el terminal de votación antes de que se lleve a cabo el cifrado del voto. Este ataque se puede llevar a cabo insertando software malicioso en el terminal de votación, por ejemplo en el ordenador del votante. Por su parte, los esquemas de papeletas precifradas logran la privacidad de los votantes incluso frente a ataques de inserción de software malicioso en el ordenador del votante, ya que los votos son escogidos a través de un código de votación que no revela información de la opción escogida por el votante. Además, los esquemas de papeletas precifradas proporcionan algunas ventajas adicionales enfocadas en la verificación de los votos. Bajo un esquema de papeletas precifradas que utiliza códigos de verificación, el votante puede asegurarse que su voto ha sido recibido correctamente por el servidor de votación. Sin embargo, los esquemas de papeletas precifradas propuestos a la fecha no permiten el

votante verificar de una manera eficiente que su voto ha sido incluido correctamente en el escrutinio de los votos. Por otro lado, los esquemas de papeletas precifradas presentan algunos retos, especialmente relacionados con la generación de las papeletas y la distribución de las mismas a los votantes.

En el capítulo 5 se describieron los actuales sistemas de registro de votantes. Dichos sistemas tienen algunas deficiencias que pueden facilitar la usurpación de la identidad de votantes. Estas deficiencias están relacionadas principalmente con la precisión en la identificación de los votantes, con la posibilidad de múltiples registros por votante y con la manipulación de la información de registro de un votante. En este capítulo se propuso un esquema de registro de votantes que hace uso de criptografía y técnicas biométricas para incrementar la precisión en la recopilación de la información de votantes a través de medios remotos. Se ha presentado una solicitud de patente internacional de dicho esquema y de las implementaciones posibles [PMV07a]. Además, el esquema ha sido presentado y publicado en [MPS08].

En el capítulo 6 se presentaron los diferentes mecanismos que permiten al votante verificar la integridad de su voto. Se analizaron los sistemas de verificación independiente propuestos en [VVSG06] y se ha concluido que, con la excepción de los sistemas de verificación con cifrado extremo a extremo, no es posible implementarlos de manera eficiente en el voto electrónico remoto. También se han analizado las propiedades de verificación de un tablón de anuncios electrónico y de los esquemas de papeletas precifradas, los cuáles son apropiados para implementaciones de voto electrónico en entornos remotos.

Además en dicho capítulo se presentaron dos aportaciones enfocadas a la verificación individual. La primera de ellas consiste en un recibo de votación criptográfico que puede sea adaptado a diferentes esquemas remotos de votación. La definición y características de dicho recibo criptográfico han sido publicadas en [MSM+08]. El recibo de votación cumple con las características esenciales de seguridad que le permiten al votante verificar la inclusión de su voto en el escrutinio. La segunda aportación presentada en el capítulo 6

consiste en un esquema de verificación basado en papeletas precifradas. El esquema propuesto cumple con los dos aspectos de verificación individual (registro y escrutinio correcto), que se consideran necesarios para que un sistema de votación sea fiable. Este esquema de votación ha sido presentado para su revisión en la revista "Computer Communications".

En el capítulo 7 se presentó un esquema que facilita la consolidación segura de resultados de un proceso electoral, aplicable tanto a entornos de voto presencial como remoto e incluso a elecciones en las que se utiliza una diversidad de canales de votación de manera simultánea. La consolidación de resultados se lleva a cabo mediante el uso de técnicas y procedimientos que permiten proteger la integridad de los resultados. El esquema propuesto describe diferentes niveles de consolidación. En cada uno de esos niveles se genera una prueba de validación que incluye información de los resultados intermedios y de la identidad de los oficiales de la elección que validaron dichos resultados. De esta manera un módulo de consolidación puede verificar que los resultados recibidos provienen de los oficiales correspondientes a la unidad electoral. Por otra parte, el módulo de consolidación genera y envía a la unidad electoral una prueba de recepción que permite a los oficiales de dicha unidad comprobar que los resultados enviados se han recibido sin ninguna manipulación. Se ha presentado una solicitud de patente internacional de dicho esquema en dónde se describe una variedad de implementaciones posibles [PMV07b].

Finalmente, en el capítulo 8 se analizaron los métodos de auditoria para los diferentes sistemas de votación. Se analizó la forma en que los sistemas de verificación independiente podrían facilitar la auditoria de un sistema de voto electrónico presencial. Se describe también porqué para un sistema de voto electrónico remoto resultaría inviable hacer uso de alguno de los sistemas de verificación independiente con fines de auditoria. En dicho capítulo se presentó un mecanismo que permite la detección de ataques de inserción de votos, es decir, en los que se añaden votos de manera ilegítima para ser parte del escrutinio. Tal como se ha mencionado previamente, en el capítulo 6 se describió la manera en que los votos, de manera individual, pueden ser verificados por los votantes

con el fin de asegurar que dichos votos se incluyen correctamente en el escrutinio. Con dichas verificaciones se puede detectar si se han eliminado o manipulado votos legítimos. Por su parte, en la propuesta presentada en el capítulo 8 se describió una forma de verificar que en el escrutinio solamente se han incluido los votos que se han emitido por votantes legítimos. Por lo tanto, dicha propuesta de auditoria en combinación con las técnicas de verificación individual propuestas en el capítulo 6, permiten ofrecer la transparencia que necesita un sistema de voto electrónico remoto. Esta transparencia es indispensable para que un sistema de votación sea fiable para todos los participantes en la elección, es decir, votantes, autoridades de la elección, candidatos, etc.

Bibliografía

[Ab98] Abe, M. "Universally verifiable MIX net with verification work independent of the number of MIX centers". Eurocrypt 98, Springer Verlag LNCS # 1403, pp. 437-447, 1998.

[Ab99] Abe, M. "Mix-networks on permutation networks". ASIACRYPT 99, Springer Verlag LNCS #1716, pp. 258-273, 1999.

[Ac04] Acquisti, A. "Receipt-free homomorphic elections and write-in ballots". Cryptology ePrint Archive, Report 2004/105, 2004.

[Ad08] Adida, B. "Helios: Web-based Open-Audit Voting". Proceedings of the 17th USENIX Security Symposium (Security '08), San Jose, CA, Jul 2008.

[ADG+00] Adler, J., Dai, W., Green, R., Neff, A. "Computational details of the votehere homomorphic election system". Technical report, Vote-Here Inc, 2000.

[AHR07] Alvarez, R.M., Hall, T.E., Roberts, B.F. "Military Voting and the Law: Procedural and Technological Solutions to the Ballot Transit Problem". Institute of Public and International Affairs, 16, 1-59, 2007.

[AI03] Abe, M., Imai, H. "Flaws in some robust optimistic Mix-Nets". Advances in Cryptology—ACISP 03, pp. 39–50, 2003.

[APR08] Aslam, J., Popa, R., Rivest, R. "On auditing elections when precincts have different sizes", 2008. Disponible electrónicamente en http://www.usenix.org/events/evt07/tech/full_papers/aslam/aslam.pdf.

[Au03] "e-Voting.at conducts first online election in Austria". Informe de e-Voting.at acerca del piloto llevado a cabo en el 2003. Disponible electrónicamente en http://www.e-voting.at/index.php?id=4&artikelID=19.

[Au04] "e-Voting.at election test at Austrian Federal President Election". Informe de e-Voting.at acerca del piloto llevado a cabo en el 2004. Disponible electrónicamente en http://www.e-voting.at/index.php?id=4&artikelID=38.

[Au06] "e-Voting Test in Cooperation with Wiener Zeitung". Informe de e-Voting.at acerca del piloto llevado a cabo en el 2006. Disponible electrónicamente en http://www.e-voting.at/index.php?id=4&artikelID=53.

[Be06] Benaloh, J. "Simple Verifiable Elections". EVT'06, Proceedings of the First Usenix/ACCURATE 348 17th USENIX Security Symposium USENIX Association Electronic Voting Technology Workshop, August 1st 2006, Vancouver, BC, Canada, 2006. Disponible electrónicamente en http://www.usenix.org/events/evt06/tech/.

[Be96] Benaloh, J. "Verifiable Secret-Ballot Elections". PhD thesis, Faculty of Graduate School, Yale University, 1996.

[BFP+01] Baudron, O., Fouque, P., Pointcheval, D., Stern, J., Poupard, G. "Practical multi-candidate election system". Twentieth Annual ACM Symposium on Principles of Distributed Computing, pp. 274–283, 2001.

[BG02] Boneh, D. and Golle, P. "Almost entirely correct mixing with applications to voting". 9th ACM Conference on Computer and Communications Security—CCS 02, pp. 68–77, 2002.

[BSL06] Biometric System Laboratory - University of Bologna: "FVC2006: The Fourth International Fingerprint Verification Competition," 2006. Disponible electrónicamente en http://bias.csr.unibo.it/fvc2006/default.asp.

[BT94] Benaloh, J., Tuinstra, D. "Receipt-free secret-ballot elections". Proceedings of the Twenty-Sixth Annual ACM Symposium on the Theory of Computing, pp. 544–553, 1994.

[BY97] Bellare, M., Yee, B. "Forward integrity for secure audit logs". Tech. rep., UC at San Diego, Dept. of Computer Science and Engineering, Nov. 1997

[Ca00] California Internet Voting Task Force. (2000). Final report. Disponible electrónicamente en http://www.ss.ca.gov/executive/ivote/.

[Ca06] Cappelli, R. "Performance evaluation of fingerprint verification systems". IEEE Trans. Pattern Anal. Mach. Intell., vol. 28, no. 1, pp. 3–18, January 2006.

[CC97] Cranor, T., Cytron, R. “Sensus: a security-conscious electronic polling system for the internet”. Proceedings of the Hawai`i International Conference on System Sciences, January 7-10, 1997.

[CdG03] Republique Et Canton De Geneve. “E-voting”. Disponible electrónicamente en http://www.geneve.ch/evoting/english/welcome.asp.

[CESG02] CESG (Communications and Electronic Security Group). "e-voting security study" 2002. Disponible electrónicamente en http://www.edemocracy.gov.uk/library/papers/ study.pdf.

[CFS+96] Cramer, R., Franklin, M., Schoenmakers, B., Yung, M. “Multi-authority secret-ballot elections with linear work”. Proc. of Eurocrypt'96, LNCS 1070, pp. 72-83,1996.

[CGS97] Cramer R., Gennaro R., Schoenmakers B. “A Secure and Optimally Efficient Multi-Authority Election Scheme”. Advances in Cryptology - EUROCRYPT '97, Lecture Notes in Computer Science, Springer-Verlag, vol. 1233, pp. 103-118, May 1997.

[Ch01] Chaum, D. “Sure Vote. Techinical Overview”. Disponible electrónicamente en http://www.vote.caltech.edu/wote01/pdfs/surevote.pdf.

[Ch04] Chaum, D. "Secret-Ballot Receipts: True Voter-Verifiable Elections". IEEE Security and Privacy, vol. 2, no. 1, pp. 38-47, Jan., 2004

[Ch81] Chaum, D. “Untraceable electronic mail, return addresses and digital pseudonyms”. Communications of the ACM, 24(2). pp. 84-88, 1981.

[Ch82] Chaum, D. “Blind signatures for untraceable payments”. Advances in Cryptology - Crypto '82, Springer-Verlag pp. 199-203, 1982.

[Ch85] Chaum, D. “Security Without Identification: Transaction System to Make Big Brother Obsolete”. Communicationf of the ACM, v. 28, n. 10, pp. 1030-1044, Oct. 1985.

[CHF08] Calandrino, J., Halderman, A., Felten, E. “In Defense of Pseudorandom Sample Selection”. USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '08), 2008.

[CHI+08] Clarkson, M., Hay, B., Inge, M., Shelat, A., Wagner, D., Yasinsac, A. “Software Review and Security Analysis of Scytl Remote Voting Software”.

Sep. 2008. Disponible electrónicamente en http://election.dos.state.fl.us/voting-systems/pdf/FinalReportSept19.pdf.

[Co07] COMELEC. "Internet Voting Electoral Board Convened". Disponible electrónicamente en http://comelec.wordpress.com/2007/08/08/internet-voting-electoral-board-convened/

[CWD06] Cordero, A., Wagner, D., Dill, D. "The role of dice in election audits"—extended abstract. IAVoSS Workshop on Trustworthy Elections 2006.

[DJ01] Damgard, I. and Jurik, M. "A Generalisation, a Simplification and some Applications of Paillier's Probabilistic Public-Key System". Public Key Cryptography-PKC 01, pp. 119–136, 2001.

[DoD06] Department of Defense U.S. Report on IVAS 2006, As Required by Section 596 of the National Defense Authorization Act for Fiscal Year 2007, December 2006.

[EC07] The Electoral Commission. "Key issues and conclusions". May 2007 electoral pilot schemes. Disponible electrónicamente en: http://www.electoralcommission.org.uk/__data/assets/electoral_commission_pdf_file/0015/13218/Keyfindingsandrecommendationssummarypaper_27191-20111__E__N__S__W__.pdf

[El07] Election Law Blog. "The Extremely Weak Evidence of Voter Fraud in Crawford, the Indiana Voter ID Case". May, 2007. Disponible electrónicamente en http://electionlawblog.org/archives/008378.html

[El08] Electoral Commission' website to register to vote. Disponible electrónicamente en http://www.aboutmyvote.co.uk/register/CitzSelect.cfm?officeID=214&CFID=12799012&CFTOKEN=71181288.

[El84] ElGamal, T. "A public key cryptosystem and a signature scheme based on discrete logarithms". CRYPTO' 84, Springer-Verlag, LNCS 196, pp.10-18, 1984.

[Es05] Estonian Internet Voting. Disponible electrónicamente en http://www.vvk.ee/engindex.html#0003.

[FOC] Federal Office of Communications. "Electronic Voting". Disponible electrónicamente en http://www.bakom.admin.ch/themen/infosociety/01691/01706/index.html?lang=en.

[FOO92] Fujioka, A., Okamoto, T., Ohta, K. "A Practical Secret Voting Scheme for Large Scale Elections" Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques: Advances in Cryptology, pp. 244-251, 1992

[FPS00] Fouque, P., Poupard, G., Stern, J. "Sharing decryption in the context of voting or lotteries". In Financial Cryptography 2000, LNCS, Springer-Verlag, 2000.

[Fr03] Rendue publique le 26 septembre 2003 "QUEL AVENIR POUR LE VOTE ÉLECTRONIQUE EN FRANCE ?". Disponible electrónicamente en http://www.foruminternet.org/telechargement/documents/reco-evote-20030926.htm.

[Fu04] Furukawa, J. "Efficient, verifiable shuffle decryption and its requirement of unlinkability". Proceedings of PKC'04, LNCS 2947, Springer-Verlag, pp. 319-332, 2004.

[Fv06] Federal Voting Assistance Program - U.S. Department of Defense. Appendix B, Electronic Transmission of Election Materials. Voting Assistance Guide, 2006. Disponible electrónicamente en http://www.fvap.gov/pubs/vag/pdfvag/appendix_b.pdf.

[FVAP08] FVAP Voting Assistance Guide. Disponible electrónicamente en http://www.fvap.gov/pubs/vag.html#ch3.

[Ge01] Gerck, E. "Internet Voting Requirements". The Bell, Vol. 1 No. 7, p. 3, ISSN 1530-048X, 2001.

[Gr03] Groth, J. "A verifiable secret shuffle of homomorphic encryptions" Public Key Cryptography 2003, Springer Verlag LNCS # 2567. pp. 145-160, 2003.

[Ha04] Hawkes, P. "MD5 collision". October 2004. Disponible electrónicamente en http://eprint.iacr.org/2004/264.

[HM03] Halvorson, E., McKnown, L. "Johnson County Demands Answers from ES&S. The use of uncertified software in elections has been widespread and napologetic". L.A. TIMES, November 13, 2003. Disponible electrónicamente en http://www.wishtv.com/Global/story.asp?S=1712213&nav=0Ra7LXSW.

[HMP95] Horster, P., Michels, M., Petersen, H. "Blind signatures and their relevance for electronic voting". Proceedings of the 11th annual Computer Security Applications Conference, 1995.

[Ho07] Hof, S. "E-Voting and Biometric Systems?" Electronic Voting in Europe. pp. 63-72. 2004.

[HS00] Hirt, M., Sako, K. "Efficient receipt-free voting based on homomorphic encryption". Advances in Cryptology—EUROCRYPT 00, pages 539–556, 2000.

[HS07] Helbach, J., Schwenk, J. "Secure Internet Voting with Code Sheets". E-Voting and Identity, First International Conference, VOTE-ID 2007, Bochum, Germany, October 4-5, 2007, Revised Selected Papers. Springer Verlag, ISBN 978-3-540-77492-1, pp.166-177, 2007.

[IIN01] Indrajit R., Indrakshi R., Natarajan N. "An Anonymous Electronic Voting Protocol for Voting Over The Internet" Proceedings of the Third International Workshop on Advanced Issues of E-Commerce and Web-Based Information Systems (WECWIS '01), pp.188, June 21-22, 2001.

[IRF08] Le Forum des droits sur l'internet. Disponible electrónicamente en http://www.foruminternet.org/.

[IS90] Ingemarsson, I., Simmons, G. J. "A protocol to set up shared secret schemes without the assistance of a mutually trusted party". Advances in Cryptology-EUROCRYPT'90., Springer Verlag LNCS series, pp. 266-283, 1990.

[ISO27002] ISO/IEC 27002:2005 (E). "Information technology – Security techniques Code of practice for information security management".

[Iv91] Iversen, K. "A Cryptographic Scheme for Computerized General Elections". Advances in Cryptology – Crypto' 91. Lecture Notes in Computer Science 576, Springer-Verlag, Berlin, pp. 405-419, 1992.

[Je01] Jefferson, D. "Requirements for electronic and internet voting systems in public elections". In WOTE 2001.

[JJ02] Juels A, Jakobsson M. "Coercion-resistant electronic elections". Cryptology ePrint Archive, Report 2002/165, 2002.

[JJR02] Jacobsson, M. Juels, A. Rivest, R. "Making Mix Nets Robust for Electronic Voting by Randomized Partial Checking". Proceedings of the 11th USENIX Security Symposium. pp. 339-353, 2002.

[Jo05a] Jones, D. "Chain Voting". 2005. Disponible electrónicamente en http://vote.nist.gov/threats/papers/ChainVoting.pdf.

[Jo05b] Jones, D. "Threats to Voting Systems. A position paper". Presented at the Workshop on Developing an Analysis of Threats to Voting Systems. National Institute of Standards and Technology. Gaithersburg, Maryland. October 7, 2005.

[JR07] Joaquim, R., Ribeiro, C. "Code Voting PROTECTION Agains Automatic Vote Manipulation in an Uncontrolled Environment". E-Voting and Identity, First International Conference, VOTE-ID 2007, Bochum, Germany. Revised Selected Papers. Springer 2007, ISBN 978-3-540-77492-1, pp.178-188, October 4-5, 2007.

[JRP04] Jain, A., Ross, A., Prabhakar, S. "An Introduction to Biometric Recognition". IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No.1, pp. 4-20, January 2004.

[JRS+04] Jefferson, D., Rubin, A., Simons, B., Wagner, D. "A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)". 2004. Disponible electrónicamente en http://servesecurityreport.org/paper.pdf.

[KK06] Kim, Y., Kim, Y. "System for electronically voting, counting, and examining ballots" Solicitud de patente US20060196939. 2006.

[Kl05] Klima, V. "Finding MD5 collisions on a notebook PC using multi-message modifications". International Scientific Conference Security and Protection of Information, May 2005.

[KMO01] Katz, J., Myers, S., Ostrovsky, R. "Cryptographic counters and applications to electronic voting". Advances in Cryptology—EUROCRYPT 01, pp. 78–92, 2001.

[Kr07] Krivoruchko, T. "Robust Coercion-Resistant Registration for Remote E-voting". Proceedings of the IAVoSS Workshop on Trustworthy Elections (WOTE 2007), 2007.

[KSX04] Kalera, M., Srihari, S., Xu, A. "Offline signature verification and identification using distance statistics". International Journal of Pattern Recognition and Artificial Intelligence, Vol. 18, No. 7 pp. 1339-1360. 2004.

[KV05] Krimmer, R., Volkamer, M. "Bits or Paper? Comparing Remote Electronic Voting to Postal Voting". EGOV, 2005.

[KY02] Kiayias, A., Yung, M. "Self-tallying elections and perfect ballot secrecy". Public Key Cryptography, 5th International Workshop—PKC 02, pp. 141–158, 2002.

[KZ08] Kanton Zürich. E-voting. https://evoting.zh.ch/MainPage/.

[LA04] Lu, H., Ali, A. "Prevent Online Identity Theft –Using Network Smart Cards for Secure Online Transactions," 2004 Information Security Conference, LNCS 3225, pp. 342-353, 2004.

[LBD+03] Lee, B. Boyd, C., Dawson, E. Kim, K. Yang, J., Yoo, S. "Providing receipt-freeness in mixnet-based voting protocols". Information Security and Cryptology, ICISC 2003.

[LK00] Lee, B., Kim, K. "Receipt-free electronic voting through collaboration of voter and honest verifier". JW-ISC 2000, pp. 101–108, 2000.

[LK02] Lee, B., Kim, K. "Receipt-free electronic voting scheme with a tamper-resistant randomizer". Information Security and Cryptology, ICISC 2002, pages 389–406, 2002.

[Lo08] Loeber, L. "E-voting in the Netherlands: from general acceptance to general doubt in two years". EVOTE08. Lecture Notes in Informatics. 3rd International Conference on Electronic Voting 2008. Bregenz, Austria. pp. 21-30, 2008.

[MAL04] Montgomery, M., Ali. A. M., Lu, H. K. "Secure Network Card – Implementation of a Standard Network Stack in a Smart Card –", IFIP Conf. on Six Smart Card Research and Advanced Application, 2004.

[Me02] Mercuri, R. "A better ballot box?" IEEE Spectrum Online, October 2002.

[MH08] Maaten, E. and Hall, T. "Improving the Transparency of Remote E-Voting: The Estonian Experience". Proceedings of Electronic Voting 2008 (EVOTE) Third International Workshop. Bregenz, Austria. Aug. 6-9, 2008. pp. 31-43, 2008.

[MH96] Michels, M, Horster, P. "Some remarks on a receipt-free and universally verifiable mix-type voting scheme". Advances of Asiacrypt'96, LNCS 1163, Springer-Verlag, pp. 192-204, 2000.

[MM05] Madise, U., Martens, T. "E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world". Proceedings of Electronic Voting 2006. Second International workshop. Bregenz, Austria. Aug. 2-4. 2006. pp. 15-26, 2006.

[MMP02] Malkhi, D., Margo, O., Pavlov, E. "E-voting without Cryptography". 2002. Disponible electrónicamente en http://citeseer.ist.psu.edu/malkhi02evoting.html.

[MOV01] Menezes, A., van Oorschot, P., Vanstone, S. Handbook of Applied Cryptography, volume 6 of Discrete Mathematics and Its Applications. CRC Press, 23-25 Blades Court, Deodar Road, London, SW15 2NU, UK, fifth edition, August 2001.

[MPS08] Morales-Rocha, V., Puiggalí, J., Soriano, M. "Secure Remote Voter Registration". EVOTE08. Lecture Notes in Informatics. 3rd International Conference on Electronic Voting 2008. Bregenz, Austria. pp. 95-108. 2008.

[MSM+08] Morales-Rocha, V., Soriano, M., Martínez-Peláez, R., Rico, F. "New multi-channel voting scheme: towards remote e-voting over the internet". International Journal of Electronic Governance, Volume 1, Number 2, pp. 155-17322, April 2008.

[Mu06] Mut, M. “Protocols de seguretat amb terceres parts: el problema de la confiança I la propietat de verificabilitat”. PhD thesis, Departament de Ciències Matemàtiques i informàtica, Universitat de les Illes Balears, 2006.

[NA03] Neff, A., Adler, J. “Verifiable e-voting”. 2003. Disponible electrónicamente en http://www.votehere.net/.

[NASS07] National Association of Secretaries of State. “Post election audit procedures by state”. Disponible electrónicamente en nass.org/index.php?option=com_docman&task=doc_download&gid=54.

[Ne00] Neff, A. “Conducting a universally verifiable electronic election using homomorphic encryption”. White paper, VoteHere Inc, 2000.

[Ne01] Neff, A. “Verifiable, secret shuffles of elgamal encrypted data for secure multi-authority elections”. 8th ACM Conference on Computer and Communications Security—CCS 01, pp. 116–125, 2001.

[Ne04] Neff, A. “Verifiable mixing (shuffling) of ElGamal pairs”. VoteHere document, 2004.

[NIST-05] NIST-Developing an Analysis of Threats to Voting Systems. 2005. Disponible electrónicamente en http://vote.nist.gov/threats/papers.htm

[OA00] Ohkubo, M., Abe, M. “A length-invariant hybrid mix”. Advances of Asiacrypt'00, LNCS 1976, Springer-Verlag, pp. 178-191, 2000.

[Ok96] Okamoto, T. “An electronic voting scheme”. Proceedings of IFIP'96, Advanced IT Tools, Chapman & Hall, pp. 21-30, 1996.

[Ok97] Okamoto, T. “Receipt-free electronic voting schemes for large scale elections”. Proceedings of Workshop on Security Protocols, LNCS 1361, Springer-Verlag, pp. 25-35, 1997.

[OKS+97] Ogata, W., Kurosawa, K., Sako, K., Takatani, K. “Fault tolerant anonymous channel”. Information and Communications Security ICICS'97, LNCS 1334, Springer-Verlag, pp. 440-444, 1997.

[OMA+99] Ohkubo, M., Miura, F., Abe, M., Fujioka, A., Okamoto, T. “An improvement on a practical secret voting scheme”. Information Security'99, LNCS 1729, Springer-Verlag, pp. 225-234, 1999.

[Op02] Oppliger, R., "How to Address the Secure Platform Problem for Remote Internet Voting". Proceedings of the 5th Conference on "Sicherheit in informations systemen" (SIS 2002), Vienna (Austria), vdf Hochschulverlag, pp. 153–173, October 3 - 4, 2002.

[Or08] Ordinateurs-de-Vote.org. Disponible electrónicamente en http://www.ordinateurs-de-vote.org/petition/.

[OVE05] Observatorio Voto Electrónico, Informe 2M6: "Así, no". Disponible electrónicamente en http://www.votobit.org/archivos/PruebaVotoInternet2005.pdf.

[Pa08] PalmBeachPost.com: "State postpones election certification". Sep. 2008. Disponible electrónicamente en http://www.palmbeachpost.com/localnews/content/local_news/epaper/2008/09/02/recount0903.html

[Pa99] Paillier, P. "Public key cryptosystems based on composite degree residousity classes". J. Stern, editor, EUROCRYPT'99, pages 223-238. Springer-Verlag, LNCS 1592, 1999.

[PBD+04] Peng, K., Boyd, C., Dawson, E.,Viswanathan, K. "A correct, private, and efficient mix network". Proceedings of PKC'04, LNCS 2947, Springer-Verlag, pp. 439-454, 2000.

[PMV07a] Puiggalí, J., Morales, V., Vallés, P. "Método y Sistema para la Protección de Registros de Información de Usuarios Aplicable a Procesos Electorales" Solicitud de patente internacional PCT/ES2007000599. Sep. 2007.

[PMV07b] Puiggalí, J., Morales, V., Vallés, P. "Método y Sistema para la Consolidación Segura y Auditable de Resultados de Procesos Electorales" Solicitud de patente internacional PCT/ES2007000681. Nov. 2007.

[Pe91] Pedersen, T. "A Threshold Cryptosystem without a Trusted Party". Advances in Cryptology - EUROCRYPT'91, D. Davies editor. Springer Verlag LNCS series, 1991.

[PM04] Przybocki, M., Martin, A. NIST, Speaker Recognition Evaluation Chronicles. In Odyssey: The Speaker and Language Recognition Workshop, pp. 12–22. Toledo, Spain, May 2004.

[PM07a] Puiggalí, J., Morales-Rocha, V. 2007. "Independent Voter Verifiability for Remote Electronic Voting", presented in SECRYPT 2007. Barcelona, Spain, 2007.

[PM07b] Puiggalí, J., Morales-Rocha, V. "Remote Voting Schemes: A Comparative Analysis". E-Voting and Identity, First International Conference, VOTE-ID 2007, Bochum, Germany, October 4-5, 2007. Lecture Notes in Computer Science 4896 Springer, ISBN 978-3-540-77492-1, pp.16-28, 2007.

[Qv05] Qvortrup, M. "First past the Postman: Voting by Mail in Comparative Perspective". The Political Quarterly 76 (3), pp. 414–419, 2005.

[RB04a] Reniu, J., Barrat, J. "Legal and Social Issues in Electronic Voting. Report on the Catalan Essays during the Elections of November, 2003" en Julian Padget / Ricardo Neira / Juan Luis Díaz de León (eds.) e-Government and e-Democracy, (Col. "Research on Computing Science" - 8), México DF, Instituto Politécnico Nacional, pp. 129-137. ISBN: 970-36-0152-9. 2004.

[RB04b] Reniu, J., Barrat, J. "Democracia electrónica y participación ciudadana. Informe sociológico y jurídico de la Consulta Ciudadana Madrid Participa", Madrid: Ayuntamiento de Madrid ISBN: 84-688-9210-6, 2004.

[RB99] Riera, A., Borrell, J. "Practical approach to anonymity in large scale electronic voting schemes". Network and Distributed System Security Symposium—NDSS 99, pp. 69–82, 1999.

[RP04] Riera, A., Puiggalí, J. "Pnyx Software Requirements Document". Documento técnico de Scytl Secure Electronic Voting. 2004.

[Re05] Reynolds, D. "The 2004 MIT Lincoln laboratory speaker recognition system". Proc. IEEE Int. Conf. Acoustics, Speech, Signal Processing, Philadelphia, PA, March 2005.

[Re08] Republique Et Canton de Geneve. "E-Voting". Disponible electrónicamente en http://www.geneve.ch/evoting/english/welcome.asp.

[RFC06] RFC 4648. October 2006. Disponible electrónicamente en http://tools.ietf.org/html/rfc4648#section-6

[Ri06a] Rivest, R. “The threeballot voting system”. Sep. 2006. Disponible electrónicamente en http://theory.csail.mit.edu/~rivest/Rivest-TheThreeBallotVotingSystem.pdf .

[Ri06b] Rivest, R. “On estimating the size of a statistical audit” 2006. Disponible electrónicamente en http://people.csail.mit.edu/rivest/Rivest-OnEstimatingTheSizeOfAStatisticalAudit.pdf.

[Ri08] Rivest, R. “A sum of square roots (SSR) pseudorandom sampling method for election audits”. April 2008. Disponible electrónicamente en http://people.csail.mit.edu/rivest/Rivest-ASumOfSquare RootsSSRPseudorandomSamplingMethodForElectionAudits.pdf.

[RRB00] Riera, A., Rifá, J., Borrel, J. “Efficient construction of vote-tags to allow open objection to the tally in electronic elections”. Elsevier. Information Processing Letters, pp. 211-215. 2000.

[Ru01] Rubin, A. “Security Considerations for Remote Electronic Voting over the Internet”. Proceedings of the 29th Research Conference on Communication, Information and Internet Policy (TPRC2001), October 2001.

[Ry04] Ryan, P. “CS-TR: 864 A Variant of the Chaum Voter-verifiable Scheme”. School of Computing Science, Newcastle University, Oct 2004.

[Sa94] Sako, K. “Electronic voting scheme allowing open objection to the tally”. IEICE Trans. Fund. of Electronics, Comm. Comp. Sci. pp. 24-30, 1994.

[Sc00] Schoenmakers, B. “Fully auditable electronic secret-ballot elections”. XOOTIC Magazine, July 2000.

[Sc03] Scott, A. “Web based voting tracking and reporting system”. Patente US7044375. 2003.

[Sc06] Schweisgut, J. “Coercion-resistant electronic elections with observer” 2nd International Workshop on Electronic Voting, Bregenz, August 2006.

[Sc08a] Schneier, B. “The Psycologhy of Security”. Jan. 18, 2008. Disponible electrónicamente en http://www.schneier.com/essay-155.html

[Sc08b] Scytl Secure Electronic Voting. “Okaloosa Distance Balloting Pilot: Security Analysis”. 2008.

[Sc96] Schneier, B. Applied Cryptography. John Wiley & Sons, 605 Third Avenue, New York, N.Y. 10158-0012, third edition, 1996.

[Sc99] Schoenmakers, B. "A simple publicly verifiable secret sharing scheme and its application to electronic voting". In Advances in Cryptology- CRYPTO, 1666 of Lecture Notes in Computer Science, pp.148–164, 1999.

[SD04a] Storer, T., Duncan, I. "Practical remote electronic elections for the UK". Privacy, Security and Trust 2004 Proceedings of the Second Annual Conference on Privacy, Security and Trust, S. Marsh, Ed., National Research Council Canada. Fredericton, New Brunswick, Canada: University of New Brunswick, pp. 41–45, October 2004.

[SD04b] Storer, T., Duncan, I. "Polsterless remote electronic voting". Journal of E-Government, 1(1) pp. 75-103, October 2004.

[SD05] Storer, T., Duncan, I. "Two variations of the mCESG pollsterless e-voting scheme". Randal Bilof, editor, COMPSAC 05 The 29th Annual International Computer Software & Applications Conference, pp. 425-430, Edinburgh, Scotland, IEEE Computer Society, July 2005..

[SDC+08] Sandler, D., Derr, K., Crosby, S., Wallach, D. "Finding the evidence in tamper-evident logs". Proceedings of the 3rd International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'08), 2008

[Sh79] Shamir, A. "How to share a secret". Communications of the ACM 22,11 pp. 612-613, 1979.

[SK94] Sako, K., Kilian, J. "Secure voting using partially compatible homomorphisms". Advances in Cryptology—CRYPTO 94, LNCS 839, pp. 411–424, 1994.

[SK98] Schneier, B., Kelsey, J. "Cryptographic support for secure logs on untrusted machines". Proceedings of the 7th conference on USENIX Security Symposium, San Antonio, Texas, January 26-29, 1998.

[SLD06] Storer, T., Little, L., Duncan, I. "An exploratory study of voter attitudes towards a pollsterless remote voting system". David Chaum, Ron Rivest, and Peter Ryan, editors, IaVoSS Workshop on Trustworthy Elections (WOTE 06) Pre-Proceedings, pp. 77-86, June 2006.

[SS04] Shubina, Anna M. and Smith, Sean W. "Design and Prototype of a Coercion-Resistant, Voter Verifiable Electronic Voting System," Proceedings of the Second Annual Conference on Privacy, Security and Trust. University of New Brunswick Fredericton, New Brunswick, Canada, October, 2004.

[St06] Stanislevic, H. "Random auditing of e-voting systems: How much is enough?". 2006. Disponible electrónicamente en www.votetrustusa.org/pdfs/VTTF/EVEPAuditing.pdf.

[St08a] Stark, P. "Election audits by sampling with probability proportional to an error bound: Dealing with discrepancies" 2008. Disponible electrónicamente en statistics.berkeley.edu/~stark/Preprints/ppebwrwd08.pdf.

[St08b] Stark, P. "Conservative Statistical Post-Election Audits" Annals of Applied Statistics in press, 2008. Disponible electrónicamente en http://works.bepress.com/philip_stark/2.

[Ti06] Tiltont, C. "The Role of Biometrics in enterprise Security". Dell Power Solutions. 2006. Disponible electrónicamente en http://www.dell.com/downloads/global/power/ps1q06-20050132-Tilton-OE.pdf.

[UEG01] Uría, P., Espinoza, J.K., Goirizelaia, I. "Sistema de voto democrático desde cualquier acceso a Internet". XVI Simposium Nacional De la Unión Científica Internacional de Radio, URSI'01. Madrid, 2001.

[Uh05] Uhlmann, C. "Polls Apart". Australian House of Representative Magazine, Issue 24, August 2005.

[Uk07a] New pilot schemes will help people vote more conveniently at the Local Government Elections in thirteen local authorities in England in May 2007. Disponible electrónicamente en http://nds.coi.gov.uk/environment/fullDetail.asp?ReleaseID=260071&NewsAreaID=2&NavigatedFromDepartment=True

[Uk07b] U.K Pilot Schemes, May 2007. Disponible electrónicamente en http://www.electoralcommission.org.uk/elections/pilotsmay2007.cfm

[Us07] United States Department of Defense. "Expanding the Use of Electronic Voting Technology for UOCAVA Citizens". May 2007.

[Ur00] Urien, P. "Internet card, a smart card as a true Internet node," Computer Communications, vol. 23, pp. 1655-1666, October 2000.

[Vo08] VoteHere. "Mail-in Ballot Tracker". Disponible electrónicamente en http://www.votehere.com/ballottrackermailin.php

[VOI00] Voting over the Internet (VOI) Voting Project, 2000. Disponible electrónicamente en http://www.fvap.gov/services/voi.html.

[VVSG06] Voluntary Voting Systems Guidelines 2005. Electoral Assistance Commission. Publicado en Feb. 2006. Disponible electrónicamente en http://www.eac.gov/voting%20systems/docs/vvsgvolumei.pdf/attachment_download/file

[VW98] Vedder, D., Weikmann, F. "Smart Cards –Requirements, Properties, and Applications". 1998.

[VZ05] Voutsis, N., Zimmermann, F. "Anonymous code lists for secure electronic voting over insecure mobile channels". Proceedings of Euro mGov 2005, Sussex University, Brighton, U.K., 10-12 July 2005.

[Wa05] Wang, X. "Cryptanalysis of the hash functions MD4 and RIPEMD". Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, vol. 3494 of Lecture Notes in Computer Science, Springer, pp. 1-18, 2005.

[WY05] Wang, X., Yu, H. "How to break MD5 and other hash functions". Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, vol. 3494 of Lecture Notes in Computer Science, Springer, pp. 19-35, 2005.

[XS06] Xia, Z., Schneider, S. "A new receipt-free e-voting scheme based on blind signature (abstract)". Proceedings of Workshop on Trustworthy Elections (WOTE 2006), pp. 127-135, Cambridge, 2006.

[YB08] Yasinsac, A., Bishop, M. "The Dynamics of Counting and Recounting Votes" Security & Privacy, IEEEVolume 6, Issue 3, pp. 22 – 29, May-June 2008.

[YJX07] Yu, Q., Jianzhuang, L., Xiaoou T. “Offline Signature Verification Using Online Handwriting Registration”. Computer Vision and Pattern Recognition, CVPR '07. pp. 1-8. Jun. 2007.